HIT Policy Committee Meeting
Draft Transcript
April 21, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Good morning, everybody, and welcome to the 11th meeting of the HIT Policy Committee. This is a federal advisory committee. The public will have opportunity at the close of the meeting to make comments and the meeting summary will be posted on the ONC Web site within a week. Let me just remind members of the committee to please identify yourselves when speaking since we do have a number of people listening on the phone and on the Web.

With that we'll go around the table and introduce the members, starting on my left with Jodi Daniel.

Jodi Daniel – ONC – Director Office of Policy & Research
Jodi Daniel. ONC.

Adam Clark – Lance Armstrong Foundation – Director for Health Policy
Adam Clark. Live Strong.

Charles Kennedy – WellPoint – VP for Health IT
Charles Kennedy. WellPoint.

Mike Klag – Johns Hopkins Bloomberg School of Public Health – Dean
Mike Klag. Johns Hopkins.

Neil Calman - Institute for Family Health - President & Cofounder
Neil Calman. Institute for Family Health.

Stephen Ondra, M.D. – VA – Senior Policy Advisor
Steve Ondra. VA.

Marc Probst – Intermountain Healthcare – CIO
Marc Probst. Intermountain Healthcare.

David Lansky – Pacific Business Group on Health – President & CEO
David Lansky. Pacific Business Group on Health.

David Blumenthal – Department of HHS – National Coordinator for Health IT
David Blumenthal. ONC.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Paul Tang. Palo Alto Medical Foundation.

Paul Egerman – eScription – CEO
Paul Egerman. Software entrepreneur.

Gayle Harrell – Florida – Former State Legislator
Gayle Harrell. Former state legislator from Florida.

Deven McGraw - Center for Democracy & Technology – Director
Deven McGraw. Center for Democracy & Technology.

Judy Faulkner – Epic Systems – Founder
Judy Faulkner. Epic.

Rick Chapman – Kindred Healthcare – Chief Administrative Officer/CIO/EVP
Rick Chapman. Kindred Healthcare.

Connie Delaney – University of Minnesota School of Nursing – Dean
Connie Delaney. University of Minnesota.

Christine Bechtel - National Partnership for Women & Families – VP
Christine Bechtel. National Partnership for Women & Families.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Tony Trenkle is also here. He just had to step away. Do we have any members on the telephone? All right. With that I'll turn it over to Dr. Blumenthal.

David Blumenthal – Department of HHS – National Coordinator for Health IT
Welcome, again. This is, it seems like, the next in our monthly meetings of the Health Information Technology Policy Committee. We have a very, I think, full and interesting agenda today. Thank you, all, for being here. Thank you for the folks on the phone and in the room. We will get later on from Tony an update on some of the regulatory work that we're doing, but in the meantime I think it would be useful for us to jump right into the agenda on the subject of meaningful use, but before I do that I should give Paul, in our usual ritual here, a chance to actually go over the agenda that's in front of us.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
All right. Thank you, David. Before I do that, so I don't forget, you have the minutes from the previous meetings that you received earlier. I wanted to see if there were any corrections to that or updates. If there are not, is there a motion to approve those?

M
Moved.

W
Seconded.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
All in favor?

Participants
Aye.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
And opposed? Abstained? Great.

Well, as David mentioned, this is going to be a very interesting agenda. We'll start out with some summary points from yesterday's hearing, which was really interesting. It was a hearing on patient and consumer engagement. Then talk about the Certification/Adoption Workgroup's recommendations

related to EHR safety, a very interesting and just a challenging area. I think there are some good recommendations to be brought forward.

Following lunch, we'll talk about another challenging and interesting area, which is privacy and security. There are just so many issues to go over and they're working on some tough ones, like consent requirements. Then the NHIN Workgroup will continue in their dialogue on the policies related to NHIN and developing a trust framework. Then we'll conclude with an update from Tony on the ongoing work of the regulations and the 2,000 comments they've had on the NPRM.

So with that, we'll start with the Meaningful Use Workgroup, which had, as I mentioned, a very interesting – we've been going on a series of hearings to look at all of the categories as we update the 2013 and 2015 criteria for meaningful use and this week we talked about the category two, which is engaging patients and their families. If I were to give a few over-arching kind of themes one might be the academic version, which is in alerting health systems we really have to make sure that we involve and address the patients' needs. A more political way to summarize might be it's the patient, stupid. Finally, there's just the direct way that one testifier summarized it, which was, "Give us the data, damn it." That probably does a good job of starting us off in terms of what we heard.

The way we began the hearing, the first group was a lot about the graphic approaches. We had a couple of patients on the panel. One of them, Regina Holliday, just got down and said, "Listen. It's time we stopped being incremental." In fact, she was responding to an ad that appeared. She just said, "There's just too much urgency to get the data to the patients and we need to move beyond the status quo." That was really a good way of starting out the hearing and it sort of continued in that vein.

There was a lot of endorsement of the criteria; one out of four clinical criteria is to engage the patients and their family. All of the panelists appreciated that. There was a unanimous and unbashful demand for universal and immediate access to their data. It was just all about patients. They have a right. They have needs. They are seeking innovators to help them use and understand that data.

Neil summarized an observation he had. We talk about privacy and security as being sort of this foundational, wrap-around issue that involves everything that we do, but as he was listening to the testimony he said that when you think of what these patients are saying that's the wrap-around cause. So that wraps around the quality of safety, efficiencies, disparities, engagement, population health, etc. So that was an interesting observation.

Another, I think Deven may have said this is sort of re-orienting in the sense of maybe what we should do is be focusing the meaningful use requirements around the patients and what's meaningful for them. So, for example, when we talk about measuring outcomes, a lot of it sort of health professional or health system focused, but what if it were the outcomes important and known to the patients, like are they alive or not? Like, what's their experience? What's the quality of life? Boy, that would change things about the end of life, etc. and one of my favorites came from Carol Raphael, which is what about the outcome of can I make it to my granddaughter's wedding? These are the views from the patients and that's a really good way to wrap around some of the outcomes that we want to have from our whole program.

Again, Carol Raphael, who's the CEO of the Visiting Nurse Association in New York, described, first of all, they see something like 35,000 visits per day, which is just tremendous. But one of the things they do using HIT is to bring, I think it's a tablet to the patient's home and review even through video, multimedia, what are they trying to teach this patient. How are they trying to educate the patient? At the end we talked about the theory of tell them what you're going to tell them, tell them, and then test whether they understand. Well, they have a test on the computer and so they test the understanding.

So when you think about it, I mean one of the key problems is the readmission rate. Well, they make sure they get out there within a couple of days of discharge. That's the teachable moment. As we all know, nowadays we kick people out of the hospital and they just need a whole lot more right after.

So the three Es that Carol talked about were, one, engagement; two, education; and three, empowerment. Those are not all wrapped up in one. They're different goals for doing things for and with patients. Again, another kind of an outcome that I think we should be measuring ourselves against and what we accomplish with this program.

Deven again talked about how in stage one criteria we had a lot of prescriptive kinds of criteria. You've got to have CPOE. You have coded data, etc. Maybe as we get information into the record and reflect more of what the patients need, stages two and three may be a little bit more outcomes oriented and less prescriptive and that would allow for innovation to serve the needs of the patients.

One of the ways in our Strategic Planning Workgroup we're talking about how do we communicate the message, what are we trying to do, how are we trying to do it, etc. and an idea came up, I think from Eric Dishman was a meaningful use video. He headed up a group called CAST and I'm not going to remember; Center for Aging Services and Technology or something like that; it's dealing with the health needs of seniors and using technology to do that, but scenarios that say what would life look like, different? How would it look different if we had this kind of support? That's not just technology support. It's human support as well.

So, finally, I think Chris Gibbons used a quote from Michael Angelo, which may be germane to all of our work, including the meaningful use work in particular, which was the greater dangers for most of us lies not in setting our aim too high and falling short, but in setting it too low and meeting them. That seems very apropos to the work of ONC and the meaningful use program and criteria in particular. Anyway, as you can tell a very full, productive and very stimulating day we had yesterday.

We are, obviously, going to come back and present to you further summaries and some recommendations, not final recommendations because this is all input into the future criteria, but some more of our reactions and digested thought we'll bring next month. Any questions on that? Not that we have any recommendations there.

The next topic I want to open up from the Meaningful Use Workgroup is Neil Calman's discussion of a topic of importance to him and the Workgroup, which is on disparities in healthcare.

Neil Calman - Institute for Family Health - President & Cofounder

Thank you, Paul. I had mentioned to Paul and he suggested that we bring it up for discussion, the idea of having a full-day hearing on the issue of disparities populations and the impact that our work is having and will have on them. I've been getting some feedback. Others have been getting some feedback and I think it's really important. Yesterday we heard some comments specifically addressing how people who are homeless, how people who are shifted on and off Medicaid, how people who are forced to change their primary care providers because of loss of insurance and others are impacted by what's really our increasing dependence on health information technology and one of the things that's so clear is as we're moving forward with this technology more and more of our system will depend upon it and the history of health disparities in this country is basically that people who are poor and people who are uninsured, mostly people of color in this country, people who live in remote, rural areas are the last to benefit from technological advances, whether they're MRIs or whether they're cardiac bypass surgery or whatever it is. This technological advance, I think we have a responsibility to make sure that that doesn't happen again

and I think the way to do that is to hear from people and to make sure that we're paying attention to those issues.

So I think there are different ways in which these disparities can play out. They can be disparities based on disabilities. How does this play out for people who are visually impaired? What does it mean if we're transferring all of this information around and we leave a population out that can't participate in it? What does it mean for people who don't have access to computers or high speed Internet in their homes when we're depending upon this as a new way of communication? Does it mean that those people won't have access to this? What do they need? What do we need to pay attention to in terms of trying to make sure that all of that happens? So my suggestion was to put together a day of hearings similar to what we had yesterday with programs that would deal with some of these issues, looking at how our work will impact on populations, who are not as fortunate as some of us are in being able to access all of this stuff.

Paul reminded me that all of us put a tremendous amount of time into the work of the Policy Committee and so I am sensitive to the fact that we're asking for a full day of additional activity, but I think that as we put this agenda together there will be many, many issues that will come to the forefront that we need to deal with and I think it deserves a day.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Thank you, Neil, for highlighting it. I strongly support our doing that. I think it goes all of the way back to the original statute that brings us here. I know in California doing the state HIE planning work there's been a very good workgroup dealing with some of those same issues and I for one was very enlightened and troubled by what they began to discuss and talk about. So I think there are many ramifications of the issue you're raising and we should understand them fully and then make sure that the work we do going forward tries to address them where we can. Tony?

Tony Trenkle – CMS – Director of OESS
Yes. Thank you very much for bringing this forward and strongly endorse it. I think given Paul's summary of the dialogue yesterday it's absolutely essential to live out the patient and family voice in its fullest.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
It sounds like a terrific idea. There is, of course, as David said, plenty of basis for this and in the HITECH legislation. There's also a very heavy emphasis in the health reform legislation on disparities reduction. It's one of our key objectives in our meaningful use framework and certainly deserves a lot of attention. There's been a modest amount of research on this question and it's not as straightforward as you might think. One of the factors that I think we'll have to track carefully is the way in which health reform at large is going to affect this issue on many, many levels. As a matter of fact, not to add too much to the agenda of this group, though it's possible to keep adding almost without limit, but I think at some point we should come back and look at how the passage of health reform should affect our thinking about our responsibilities and the intersection.

Just one relatively minor, not minor; very important, but easy to overlook; factor that could affect disparities is the huge investment that health reform is making in the community health centers and the opportunity that that may give health centers to address some of the disparities that we've been talking about.

Christine Bechtel - National Partnership for Women & Families – VP
Yes. I completely agree; this is Christine Bechtel; with both and I would say with respect to the ... disparities hearing there are a couple of us on the meaningful use workgroup, who are also on the strategic plan workgroup and I think it's incumbent upon us to make sure that as the strategic plan work

moves forward that we're really lifting that out of the plan in a way that is strategic and ensures that we recommend to you the right focus in terms of the strategic work that goes forward. On the health reform side, I think that's enormously important and maybe we can do those back-to-back.

David Blumenthal – Department of HHS – National Coordinator for Health IT
Paul, do you want to take us to the next agenda item?

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Sure. The next agenda is to look at the recommendations coming forth by the Certification/Adoption Workgroup on EHR safety. Paul Egerman and Marc Probst are leading that. I just want to note for the committee members that Jeff Shuren from the FDA is going to be on-line listening to this and would like to make a couple of comments after the folks have presented, after Marc and Paul have presented their recommendations and reports.

Paul Egerman – eScription – CEO
Great. Thank you. Good morning. I'm Paul Egerman and I'm here to present the second part of our recommendations regarding this issue of patient safety. At the last meeting, March 19th, we presented preliminary recommendations. We received feedback from you all. We received feedback from the public. We had two subsequent conference calls and so we're ready to present now what we hope is our final recommendations, which are in the form of a letter in the materials.

Basically, what I'm going to do is quickly review the workgroup itself. I'm going to also very quickly review a little bit of the hearing to remind you of some of the major learnings we got from that and then talk about how our recommendations have changed.

These are the members of the workgroup listed on the screen. I feel badly in some sense just listing the members and going through it so fast. These people have done really an extraordinary job, because we've actually put them on a parallel track. Not only have we worked on this very interesting issue of patient safety, but we've also been working on the certification NPRM and so we've had meetings like every week or two and an absolute torrent of e-mails. This group has really done a terrific job, so I wanted to say thank you to the group.

I also want to thank our presenters. These people presented at our February 25th hearing and what is particularly interesting is not only did they present at the hearing, but they also continued to stay involved and so they commented on all of our work documents. They listened to our workgroup conference calls and gave us feedback every step along the way and so we're very fortunate, because these are all experts in their field and we're very fortunate to have that expertise added to our work, so we appreciate what all of those people have done.

Now, to summarize the hearing, again, we did a hearing, as Dr. Tang said, on this topic of patient safety. When we talk about patient safety in this context we're really talking about it from a context of like things that go wrong, adverse impact, unexpected consequences. That was the area that we were looking at and I made this comment last time that a lot of the information that was presented appeared to be drawn from anecdotes and from the personal experiences of the presenters and also the workgroup members. I did get a little bit of pushback from some of the presenters after my presentation, who said that I perhaps stated that too starkly; that there have been some studies and so that it was not quite correct to say very little data. It might have been better to say little data though and that there is some data available. Everybody agrees that there is a clear need for a lot more investigation, however. That was a comment that I wanted to make sure I reported.

... to report that there is continued confidence in HIT. I also want to point out that this discussion that we had was about HIT, Healthcare Information Technology. It was not limited to electronic health records, so this included a lot of things in areas that we don't normally travel, so retail pharmacy systems in commercial labs, a lot of areas that were very interesting. This is also obviously an area for concern. This is a very sensitive, important and challenging issue.

That's a quick summary. Now, again, to remind you of something I said last time, when you think about this issue of adverse events or unexpected consequences one would normally first think about technology issues and think about software bugs. That's sort of like an expectation that this is all about software bugs, but what we learned was if you view it that way that view is too narrow. That's not a correct and clear description. In fact, the software bugs issue seems to be the minority of the issues. There seem to be much larger issues. The largest issue, the most interesting was this concept of the complex interactions of people and technology; that this is where there are a lot of issues coming up.

One of the members of our workgroup, Dr. Joan Ash, suggested the phrase "a socio-technical environment" to describe what is going on. The real issue is how is this technology being used in real world environments. We clearly saw that there were training and implementation issues and we clearly saw that there were interoperability issues that also impacted this area.

To give you an example of the concept of socio-technical environment is talk about the concept of alert fatigue. I think people understand what alert fatigue is. Alert fatigue is when you're ordering anything, ordering a medication, so many alerts are presented to the orderer that they end up basically ignoring like 90% of the alerts that they see. So if you end up ignoring 90% of the alerts that you see, you tend to get used to ignoring the alerts and when you start to ignore the alerts there's a risk that you're going to ignore something that's actually very important and very valuable. So that's sort of an example.

When you look at that issue of alert fatigue that's actually a very good example of how it's possible the system actually can be working correctly from a software standpoint. There's really no bugs or anything in the system, but it's the basic environment in which it is being used by humans, especially some of those people can be very, very busy and also under a lot of stress and so if they're very busy and a lot of stress that they can miss some things. That is an example of how the systems might not be fulfilling their full potential. So the main concept there again is it's not just software. It's this sort of broader category of this socio-technical environment.

Now, we made a number of recommendations and I'm here to tell you how we've updated those recommendations since last time. First is we updated our goal for how to address this issue and we basically sort of cleaned up the language and tried to make it very clear that what we're trying to do is very much consistent with the strategic plan. The goal is described in the strategic plan and the National Coordinator's vision of a learning health and healthcare system. So we want to have a patient centered approach to safety that is consistent with that concept that this is also sort of an incremental process that we will be continuing to learn and we will be continuing to approve these systems and to achieve the goal a culture of improvement needs to be created by each healthcare entity.

Then we have a number of recommendations related to this. The first group of recommendations relate to this concept of information gathering. Basically, this need to get more data, more information about what is going on; so the first one is basically this concept of a national, transparent database or information system. This is sort of like the headline news from my last presentation. I gave the example of the FAA and Captain Sullenberger, who a number of people informed me afterwards is actually a pilot and not a pirate; perhaps just a wordy mistake on my part. But basically, the concept here was to create

a database and an oversight process. The way we change this is we create greater emphasis on oversight process and on the database.

Now, when we presented last month one of the things we did was we said that we wanted this to be a patient safety organization, a PSO, which is sort of clearly defined in the legislation. Then we got a number of questions. People would say, "Can a PSO handle confidentiality?" That was a question that you had asked, Gayle. We started finding ourselves talking about what a PSO can and can't do and how to compare a PSO with what the FDA can and can't do. What we decided was that's not a place where we belong. What we wanted to do was simply say there is a need for this national database and there is this need for this oversight process and we would simply describe the attributes of what is needed. We weren't going to define how it was actually going to be implemented, because it's, actually once we started to look at it, sort of a daunting issue is to figure out how it would be implemented.

So the way this changed is to clearly indicate that we're looking at a national information system and an oversight process without specifying who's going to do that or how it's going to get done. Then we list out the attributes. The attributes are this capability to do confidential reporting, to have liability protection. An ability to investigate serious incidents, standardized database reporting, an ability to receive reports from a broad range of stakeholders, patients, clinicians, vendors, healthcare organizations, and a reporting process that covers multiple factors. So this is, again, based on the learning. It has to include usability, workflow processes, multiple factors and also a process that covers not only all of HIT, but all software sources, so it includes Open Source and self developed systems. Of course, most importantly if they could get this concept as a learning system an ability to disseminate information ... gather this information, to be able to disseminate. So these are the attributes of this information system.

Another aspect of this or primary recommendation is what you see is we call it recommendation 1.1. We wanted to get past this issue of do we really have good data here? Is this based on anecdotes? What we felt was really critically important was that there would be sort of a very thorough and authoritative and formal analysis of this entire area, so we made a recommendation that the Office of the National Coordinator commission such a formal study. We're looking for something like the Institute of Medicine Study that was done in 1999. That's the kind of evaluation that we are suggesting that needs to be done so that we have a clear evaluation that was carefully done. It was really what is the extent of these patient safety issues and also as part of that, what recommendations really need to be done? We think that is altogether an important recommendation. That's our recommendation number one.

Now we have several other recommendations. Some of these are the same as what we presented last. This first group is called facilitate and encourage reporting. Again, these are recommendations, actually, that we made last time, but we simply sort of reorganized them and categorized them so people could understand what we're trying to accomplish, because we recognize that you can put together a reporting structure and a reporting system, but that doesn't necessarily, by itself mean anybody will use it and that you need to do something to make it easier to use and to encourage reporting and so we have a number of recommendations.

One is called – it sort of sounds like a really sort of techy thing called the feedback button, which will allow a clinician, when they see a screen that's confusing or perhaps see something with incorrect data to basically sort of like have a little button that they push and they can forward information to like an IT person to review that. That actually got some fair, positive comments in the trade press. People thought that was a good idea.

We also have a recommendation that states true meaningful use require healthcare organizations and physicians to report in a timely way their information to the reporting organization. Then we have a training recommendation here. So that's to facilitate and encourage reporting.

We had a recommendation specifically for vendors. It's to address a number of issues that were discussed, but it's basically to use certification criteria to require vendors to keep track of patient safety information and also to give alerts to their customers if they are aware of a patient safety problem.

We did address the issue of patient engagement and what we wrote and changed from last time, but there is a write up as how patients could be helpful in this entire process. We also have recommendations about implementation, education and training. We wordsmithed this a little bit, but the basic concepts did not change from the previous meeting.

We have a recommendation about interoperability, which is a very interesting issue. It explains what that's all about. Our recommendation on interoperability is a recommendation actually to the standards committee, so we're asking the standards committee to do something. What it is we're asking them to do is to consider the concept of what's called traceability. You're wondering what is traceability all about as it relates to interoperability or as it relates to interfaces.

Traceability is simply a way when something goes wrong through an interface to be able to track through what was the source of the problem, because things can go through various transformations. So we talked last time about a situation that occurred at the VA where data went from one system to some middleware piece that transformed it to another system and when that occurs there is a probability of an error, so this is a recommendation that the standards committee consider traceability, which is issues like audit trails and logs of transactions.

We have a best safety practices comment and we also have a comment and recommendations about accreditation. What we want to do is we have three recommendations that are new compared to last month that I want to take you through.

The first one, a very interesting recommendation, has to do with the timing of stage two and three. This is a suggestion from the vendors, which they say is a patient safety issue. They want to make sure that when we get to stage two and stage three that they have time to develop their software and healthcare organizations have time to update their software. They're afraid that if we don't have enough time to do that there will be errors and that will be a patient safety problem.

What they are asking for is 18 months prior to the beginning of the eligibility period, 18 months to have the certification criteria finalized. So the way they get to 18 months is they say they need 12 months for vendors to develop and test and certify their software and 6 months for customers to receive it and test and train their people on it. Those numbers seem, in my opinion, reasonable. In fact, if anything, for a lot of vendors they might be very short. If you're a vendor and you have over 1,000 customers to somehow distribute this software to 1,000 people it's sort of a daunting proposition.

Now, you could look at this and say why in the world are you talking about this now? I mean the eligibility period for stage two is October 1, 2012. It seems like it's a long ways away, but if you start to back up the schedule you realize if the eligibility period starts October 1, 2012 and you want everything done in 18 months that means you'd want to have your certification criteria finalized by April 1, 2011, which may still seem like a long ways away because that's a year off. But we also have this wonderful regulatory process that we just learned a lot about and that sort of suggests to us that if you're going to get things finalized by April 1, 2011, we really have to start publishing the regs probably December of this year or

January 2011 at the latest. So that means we really put them at eight months or so of having a final picture of stage two even though we have no idea yet even what stage one looks like.

So it's an interesting timing issue. This comment and recommendation is sort of a lot different than the other recommendations. So what we might want to do is sort of carve that out and keep it … a separate discussion. What makes it different is compared to all of our other recommendations this is actually an issue that relates entirely to this group. Everything else is like the rest of the real world. This is our group and we actually have control over this issue ourselves and so it's, by itself, a very interesting issue.

Now, our next issue is also an absolutely fascinating issue. It's an issue related to the Food and Drug Administration, FDA. This is a fascinating issue. It's a surprisingly emotional issue. People have very strong opinions on this issue. I first want to make two comments before I talk a lot about it. The first comment I want to make is that Jeff Shuren and the people of the FDA have been just terrific to work with. They've been extremely helpful. They've given us data when we've asked for it. They've explained things. They've been accessible and they've said over and over again that they will be flexible on these issues. They're clearly trying very hard to be helpful.

The second comment I want to make; and Jodi, you've got to correct me if I say this wrong; but basically the FDA already has legislative authority over healthcare IT. They have the authority to regulate this entire area and they're a separate, independent agency so that our workgroup and our policy committee, at least our workgroup, the only standing we really have is just to make recommendations to ONC in terms of what their working relationship should be to FDA. It's not like we can make recommendations as to what FDA should and shouldn't do.

So those are the two comments I'd make, but despite the situation, our workgroup couldn't help itself but to talk a lot about the FDA. I mean this is just an interesting and important topic, so you see listed in your materials some of the concerns we had about the way the FDA approaches things, so really what we're trying to do with the EHR system. The first one is this concern about the focus on problems caused by individual devices. Again, if you think about the example of the alert fatigue issue where really systems are working correctly, we didn't understand how the FDA would be able to address that kind of an issue.

The second observation that we had about the FDA was their focus on serious injuries and death and basically seem to be involved in the most … like egregious violations, which is something that's certainly important from a regulatory standpoint, but one would hope that for electronic health records we would be a little bit further, sort of upstream. That we'd be dealing with hazardous conditions or unsafe conditions before there was a serious injury. That was the intention.

The third thing had to do with this process called QSR, the Quality Systems Regulation. There was concern about whether or not that was appropriate for HIT, although I understand that the FDA seemed like they're willing to be flexible on this issue.

The fourth comment is a very important comment that was raised. It was a concern that FDA regulation, especially if it went to class two regulation, would increase costs in such a way that it would become a barrier to entry for small vendors. If you look at some of the potential for innovation development, so you have this image of a modular system, you could have people who want to create systems, say, for like an iPhone that deals with medication compliance or something. iPhone applications normally sell for like $2 or $3 each and to try to layer FDA regulation onto vendors like that could make it prohibitive to develop that kind of an application, so those are the concerns.

There are also some things that were discussed on the positive side where it was very clear that the FDA has some really valuable experience and ONC should leverage. So the ability to use, to collaborate on certification criteria and the ability perhaps encourage to work with the FDA to focus on HIT areas that we perceive are creating specific safety risk could be very valuable in terms of achieving the goals we want to achieve.

So we took all of this together and the recommendation we made was our recommendation 8.0 is that the ONC needs to work with the FDA and representatives of a broad base of stakeholders, patients, clinicians, vendors, healthcare organizations to have an open discussion of all of these topics to determine the role that the FDA should play to improve the safe use of certified EHR technology.

Our final observation and recommendation actually came from the public comments that we heard at the end of the meeting on May 19th when the people spoke in public comments. They made a comment with a fair amount of passion saying the Institute of Medicine Study occurred over ten years ago and patients are dying every day because these systems aren't being implemented.

I mean you look at the concept of alert fatigue and alert fatigue is a problem and that might mean that some important alerts are being missed and maybe half of all important alerts are being missed, but if you don't implement these systems you're going to miss a whole lot more alerts. You're going to miss 100% of all important alerts if you don't implement these systems.

So this is just an observation that our workgroup did not hear any testimony from anybody that indicated that these systems should not be implemented. We would have listened to it if somebody presented it, but nobody presented that information. We clearly heard some frustrations that these systems are not reaching their full potential. There was a lot of frustration that we could see and we clearly heard that these systems need to be implemented correctly and properly, although that's true of a lot of things in medicine.

We heard that also, but we came to the conclusion that the biggest risk to patient safety would be to either avoid or delay the proper implementation of these systems, so our recommendation number nine is very simple, which is to basically stay the course. We think that ONC needs to continue its efforts to encourage implementation of the EHR systems.

So that is our presentation. I'd open up for comments, but if I heard you right, perhaps the next step is to ask if Dr. Shuren wants to speak.

M
Let me start by thanking the committee for a very thorough and comprehensive and subtle, carefully reasoned report. I'm sure there will be lots of questions, but before we take questions I hope that Jeff Shuren from the FDA is on the line.

Jeffrey Shuren - FDA
Yes, I am on.

M
Great, Jeff. We would love to hear; let me just say by echoing Paul that ONC has been in continuing dialogue with our colleagues at FDA. They are, of course, an independent agency, but Jeff and I work for the same boss, the Secretary of Health and Human Services. We're part of the same organization, so we have plenty of opportunities to talk among ourselves and so we have been actively consulting with one

another throughout this process. Jeff, did you have any comments that you'd like to make in response to the report?

Jeffrey Shuren – FDA

Yes. First, let me say thank you to the committee. We have really enjoyed our interaction with you and very much appreciate the very thoughtful dialogue we've been having throughout this entire process. I just want to make a few comments purely to provide clarity and not to advocate for any one particular position and also to emphasize, I think as was pointed out, that the agency is very willing to be flexible and be part of sort of a broader approach pertaining to health information technology.

I just wanted to address some of the concerns raised, again, just for clarity sake. To the first point about the focus on devices, just to say that when the agency identifies there is a problem or there could have been a problem with the device and we conduct a root cause analysis, we actually look beyond the technology.

We also look at the environment in which it's being used, who uses it and how it's being used because the problems that we will deal with could be something that are inherent to the device itself. It could be, particularly with software, due to the interface of that software with another system. We've seen a number of instances of a problem, not because there was anything wrong with the health information technology software, but when it connected to another system there were problems in that communication. In fact, interoperability is a big issue for FDA. We just held a large conference in February to talk about it.

A third area is the—and I like the way it's put—that sort of socio-technical environment. We talk about human factor. The interface of a person with technology, and that the technology itself might be fine, but when you link it up with a person you've got to take into consideration the characteristics of that person and their work practices. Sometimes we see troubles there and so there's a big effort on the part of the agency to look at human factors and sometimes it's just completely separate from that as well.

When we look at ways of addressing it our tools are not just focused on technology. It really also comes down to issues of training and quality assurance and safe use practices. This has been highlighted in some actions the agency has taken more recently. I'll give one example with medical imaging where those technologies if used properly are safe and what we have seen is sometimes problems with how the technology is used and the solution sometimes is to address better work practices and sometimes the technology can be redesigned to reduce the likelihood of human error.

The second thing I wanted to address was in terms of reporting. You're quite right as to our mandatory reporting. It does go to serious injury and death with the caveat that it is also for reports where there is a malfunction that may have resulted in no injury, but if it recurred could cause serious injury or death, but that's just the mandatory side. We have several different kinds of tools for getting reports and so for our voluntary system in MedWatch we actually do receive reports of minor injuries or no injuries, the near misses. In our surveillance network, our medical product surveillance network, in which healthcare facilities voluntarily sign up to be a part of the network and get special training from the agency to look for problems and report them, we actually get a lot of reports about near misses, no harm actually occurred, from those institutions. They can report to us or we can use it for a query.

Then the last thing I wanted to mention is on the quality systems. It really is a flexible approach that is tailored by the manufacturer to their particular business process and it's been designed to handle incremental innovation, which is not only the root of development for software; it's actually the root of development for all medical devices. Our industries rely on incremental innovation all of the time and our

quality systems is designed to account for that. It really focuses on a system of checks and balances in the design of, for example, software and making sure you have the right processes in place to identify if there are problems. In fact, we have put out guidance on how the QSR applies for software and we would look to; if we were in this area we can always provide more.

I'll lastly say then, in fact, some HIT manufacturers have already moved forward to start adopting the system. Again, we're not advocating for it, just use it as an example that it actually can be adaptable and flexible for the sphere of software and other kinds of HIT technology.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Great. Jeff, would you comment on the liability issue and your protections of people reporting safety problems?

Jeffrey Shuren – FDA
Certainly. What we do is when we get a report in we de-identify it. That's for both mandatory and voluntary reports to protect the identity of the reporter, the practitioner, user facility and the patient and all of that to reduce the risk of liability. Moreover, for user facility reports that pertain to device related deaths or serious injuries that are required by law, they cannot be used in civil lawsuits. That is a protection that is put in place by law. We also make very clear and we put it in our federal regulations that the submission of any information to us about an adverse event or a near miss and any release by the agency of that information doesn't reflect a conclusion on our part. That the information that was submitted is any admission that there was a problem with the device or the entity that reported the problem or of any employee who was involved with dealing with that technology.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
So have there been instances of reports leading to malpractice or any other problems related liability or retribution against reporters or anything of that sort?

Jeffrey Shuren - FDA
I don't know the answer, if it was ever used in any particular court case.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Okay. Then one other question that has to do with the data that you accumulate through reporting and what you do with it and what happens to it after you've processed it.

Jeffrey Shuren - FDA
Well, the reports themselves, when they're de-identified, are made available to the public, so in that form they're made available. We also conduct analyses on the reports and then provide our findings in some cases and recommendations out in a variety of different mechanisms up on our Web sites, directly to manufacturers, out in patient safety news, through our communications with the ... network and out through other outlets and key partners. Based upon that information we may also call together interested stakeholders in individual meetings or hold a public meeting or workshop to discuss the findings more broadly and to work together on potential solutions.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Great. Let's open it up to questions either to Paul and Marc or to Jeff. Before we do that, Marc, do you have anything you want to contribute at this point?

Marc Probst – Intermountain Healthcare – CIO
I don't. No.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Okay. Charles. Chuck.

Charles Kennedy – WellPoint – VP for Health IT
The recommendations talk quite clearly about collaboration or potential collaborations with FDA, regional extension centers, AMIA, but they don't clearly call out potential collaborations with existing quality assurance functions, like JCAHO or provider credentialing that health plans do and I was just wondering kind of where that lies in the group's thinking.

Paul Egerman – eScription – CEO
Actually, we do have a recommendation about accreditation organizations, including JCAHO. Basically what we said was that ONC should work with those organizations on this issue because that's clearly what they're supposed to be doing is dealing with patient safety and to make sure that there are things like hospitals have a patent safety committee that looks at these issues, but also it could be another vehicle to make sure that the reporting is done in a prompt way. I mean it seems like an accreditation organization would be a great vehicle to make sure that the training has occurred correctly, the clinicians know how to report issues and that the healthcare organization is reporting their issues to the national organization promptly. So I think, Charles, your question is a great one. Perhaps I just passed by that too quickly when I did my presentation, but it's a great question.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Okay. Gayle and then Deven and then Christine. We have two modes of alerting me here. There's the waving of the hand and there's the thing on its end. The problem with the thing on its end is that we have a socio-technical problem here. If you put it on its end it's going to end up in the—

(Overlapping voices.)

Gayle Harrell – Florida – Former State Legislator
We all need an easy button here. My question goes back to the interrelationship between ONC and FDA. You call out very much in your first recommendation the need for some kind of patient safety organization. Everything that you have described here kind of relates or is very much consistent with what I'm hearing from Jeff as to what the FDA is doing currently. Where do your recommendations part from what they currently do? Are they the group that should be doing this patient safety organization that you are calling out here?

Paul Egerman – eScription – CEO
That's a good question, Gayle. There is just a number of choices. I mean there are organizations called patient safety organizations. If we had a representative from one of those here he or she would say, "Yes, we can do the liability part too. We can do this part too. Here's what we do better." Our workgroup did not want to be in a position of trying to referee that yet.

We simply said, "These are the attributes of what needs to happen," and so that's where we are. We think that that's another discussion that ONC either needs to make itself or ONC needs to have some vehicle decide. They could choose a PSO. They could choose the FDA. They could choose some combination of that. They could use both of them. There are a lot of ways to do it. We didn't want to get that far down the line yet.

Gayle Harrell – Florida – Former State Legislator

Well, I have great concern that we wind up with either duplicative agencies or bureaucracies or conflicting requirements and we need to be very clear in our recommendation on how we're going to do this or what ONC is going to do so that you don't wind up with a conflict or duplication and you have hospitals, you have vendors, you have doctors having to report to several different people. So the waters get very muddied. I think we need to be very clear in the direction that we want to see this go in our recommendation.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Deven.

Deven McGraw - Center for Democracy & Technology – Director
I have a couple of questions. One is a small one. One is whether you consider Malware to be a software bug. If it's not always a bug it ought to be on the list of things that need to be looked out for.

The second thing is with respect to the patient safety organization and the FDA's process for getting reports and sort of dealing in a confidential way with those reports so that there's a culture of safety to be encouraged, but without creating additional information that can be used in a civil suit, there is a statute that establishes the patient safety organizations, that provides for all of this protection on the data and essentially if the PSO process or the FDA's process are not used as the process for which these reports are generated you can't guarantee these data protections, because Congress essentially has to establish them by pre-empting laws on civil discovery that would otherwise apply in this context.

The PSO is not a mandatory reporting organization. In many cases, and I'm not as familiar with FDA's reporting laws and I know Jeff is, FDA reports are, in some cases, mandatory. The use of a PSO is voluntary, but when you use it you do get these protections on the data, so essentially I think we'd want to make sure that whatever process ONC might decide to set up for itself could fit in within the existing statutory authority that grants to PSOs those protections on the data. I think at least I recognize and I'm seeing some heads nodding that being able to protect this data from being independently discoverable is critical to ensuring that it actually gets reported.

M
Just to follow up, to clarify, Deven, since you are a lawyer and seem to know this area; is there any distinction in the level of protection that's afforded to reporters under the FDA or the PSO process that you think that you can see?

Deven McGraw - Center for Democracy & Technology – Director
That's a good question that I don't know off the top of my head. You'd have to sort of take the set of FDA protections and match it up against the ones that are in the patient safety. I actually used to know the act by heart, but it's been a couple of years, so I don't, but you could sort of measure them up. One may be more than the other, but we worked really hard when we worked on that statute to make sure that at least with respect to what gets reported in and generated out, it's like attorney work product essentially, that that wouldn't be discoverable. But the other thing to keep in mind is if the error is independently discovered outside of the process of the root cause analysis that is the essence of PSO, that cloak of confidentiality doesn't extend to all of the data, just to whatever is part of the safety process. So if something gets independently discovered it still could be used in a suit, for example.

Paul Egerman – eScription – CEO
I was going to say Bill Munier did give us similar information to what Jeff just said in terms of the legal protections that a PSO provides. At least I decided it was above my pay grade to compare these two in terms of which provides better and what's better in what circumstances, but that certainly is a clear issue.

Deven is correct though. The PSO and the FDA do provide some level of exactly this protection that is needed in order to get the reporting to occur.

Jeffrey Shuren – FDA
Deven, when you're talking about Malware are you talking about the impacts of it and the ability to report against those impacts of Malware? What was your concern?

Deven McGraw - Center for Democracy & Technology – Director
I think just the idea of raising it as a potential safety issue that's beyond just an internal bug in the software since it comes from an external source into the software and can wreak all kinds of havoc, as we know, and for which we have sort of tools in place, antivirus software, for example, but maybe more difficult with respect to devices that are regulated where you can't make major changes to them necessarily once they've been approved, even when antivirus software might provide some sort of protection. This issue just came to us somewhat anecdotally, so I think I was only raising it just in terms of sort of the kind of list of we had the list of issues you all had on the earlier slide, which included the technical, as well as the human in combination with the technical. So, I wanted to get a sense of the scope of the technical, making sure Malware was on there.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Christine and then Judy and then Mike.

Christine Bechtel - National Partnership for Women & Families – VP
First of all, thank you, Paul and Marc and Jeff, for really terrific work in this area. Very thoughtful recommendations. My question is in the patient engagement area, which will shock you I'm sure. You talk about making it easier for patients to report inaccurate or questionable data. I think as a policy matter that's right on. I know that you heard from Dave deBronkart, who talks a lot about letting patients help in this area, so my question is how do we move that forward in a practical manner. I'm assuming that you don't have a recommendation for a reason; that maybe it's not ready for primetime, but I'm wondering how do we move it forward. Do we need to ask the standards committee to do anything? Should it be part of future meaningful use requirements, etc.?

Paul Egerman – eScription – CEO
It's a great question. First of all, the reason that that comment was there was a belief that once patients get access to their data they're going to spot some things. It's sort of the counter ... view as well. Not all patients will access their data, but you don't really need all patients to access the data. So if you've got some interoperability problem usually the way interoperability problems get resolved is that some physician spots data that's bad, but because they can't really know everything that's going on they tend to spot the most obvious things, so it's an issue like there is some gender problem. The patient is a male and it's some female test that has been performed on the person, so it's clearly wrong. When that occurs it gets written up in the newspapers too because it sort of shows that these systems look absolutely terrible; whereas if you have patients who have access, even if only 5% of the patients have access they could spot other data elements perhaps sooner so that they could help you. That's part of the concept about how patients can help as it relates to patient safety.

The concept of the feedback button is similar to the physician one. That if they had some capability when they spot something to sort of identify it and then communicate back through the source as to where the problem might be that that could be very useful. We did not, however, make a specific recommendation in that area.

The reason we didn't make a recommendation was two-fold. I mean so far the PHR itself has not been an area that certification has touched and so we didn't want to necessarily begin and open that issue. There are other issues too. What about patient portals and tethered? How does that fit in? We felt that there was this discussion yesterday that there would be a lot more discussion about patient engagement and it's better placed in part of an entire thoughtful review of that entire issue.

That was our thought process. We're certainly open to a stronger position. That's why we did it the way we did it.

Christine Bechtel - National Partnership for Women & Families – VP
Okay. Well, rather than sort of trying to come up with a recommendation on the fly it would be great if you guys could take that on in your continuing work because you're right about we're not ready for certification of PHRs. There is a lot of controversy around that. But on the other hand, there may be some other ways; whether it's a meaningful use requirement, a secure communication link that we're saying this is a policy matter. We just sort of need to figure out how do we move that forward in the market in an appropriate way. It would be great if you could continue to keep it on your radar.

Paul Egerman – eScription – CEO
Indeed. You mentioned Dave deBronkart. He was helpful in that discussion. The interesting analogy he posed was when consumers had access to the credit card bills and could easily question individual line items on the credit card bills. The credit card companies cleaned up their billing really fast.

Christine Bechtel - National Partnership for Women & Families – VP
Yes.

Paul Egerman – eScription – CEO
The sense is that's variable. We'd like the data to be right.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Judy.

Judy Faulkner – Epic Systems – Founder
I have two things too. The first is when I was on the phone once when you were having a conference call on this topic, Marc, you gave a couple minute review of all of the different ways that patient safety could be interpreted. I think it was training, operating systems, all sorts of things. I thought that was really excellent. I think it helps us understand all of the different ways you look at it. It's not just, as you said, software. It's not just software and user interface. It's a whole lot of different things. I thought it would be really helpful for this group if you could reproduce that list that you had because it was a really good list.

Marc Probst – Intermountain Healthcare – CIO
On the fly or do you want me to reproduce the list?

Judy Faulkner – Epic Systems – Founder
No. No. Not on the fly.

Marc Probst – Intermountain Healthcare – CIO
Because I can reproduce the list.

Judy Faulkner – Epic Systems – Founder
The second thing is the 18 months. I thought that's as good as any number, but I do want to bring up that a change could take a day. A change could take three years. A change for one vendor could take a very

short time. Like I know changing ID numbers from six digits to seven digits, one vendor might take a day or two on that; another vendor may take years on that. If you think of Y2K ... Y2K, people had 12 months to develop, 6 months to install? That's a good example of the sort of things that could occur.

I think that as you build that timeline, somehow there's got to be flexibility, especially if you have a large healthcare organization; even if it can be done in a number of months. If you have a large healthcare organization it affects lots of products: radiology, pharmacy, lab, nursing, ordering, everything. They have 10,000, 20,000, 30,000 employees, who all need to get the new software, need to be trained. Then you stop everything they're doing, including that new hospital they were just going to bring up with the software, I think there are all sorts of considerations that go into those 18 months. I think that a very hard line might be very difficult.

Then the third thing: On the FDA, you have in there that harms innovation. I wanted to extend that a little bit. I think what it does is it slows development and that harms innovation. It's not that it harms innovation in terms of people can't think of enough creative things. It's that the development is slowed.

The thing I wanted to point out is I was listening to a CIO talk about blood bank and he was saying that he feels that the safety of blood bank is more difficult because the vendors have to go so slow that needed changes don't get into there. The other thing I know about things such as blood bank is many of the vendors, instead of building that themselves, will interface to a third party for blood bank just because the innovation and the speed of development is so different.

So there has to be a balance that says what's the value and kind of went back to what you were saying, even with CPOE and electronic health records, everybody was saying get them out even though there may be some safety problems. Get them out because they can help more than they could hurt. I think that balance has to always be there. I think if we look into blood bank and why the vendors act a certain way and why the users react a certain way it may help us figure out how to go forward.

Paul Egerman – eScription – CEO
This is very helpful.

David Blumenthal – Department of HHS – National Coordinator for Health IT
All right, actually, David Lansky was in line and I missed it, so David next and then Mike.

David Lansky – Pacific Business Group on Health – President & CEO
Thank you. Well, I really appreciate the work of the committee. It's been very instructive for all of us I think. I only have one concern which is almost outside our scope, but the goal statement you offered emphasizes a patient-centered approach to HIT safety.

One of the strengths of our committee as a whole has been not looking at our work through the lens of technology, but looking at it through the lens of the patient and healthcare delivery. My concern is that with recommendation number one, I think there's a risk of shining the spotlight on the technology and not on patient safety. The point you made at the end, Paul, about it's been a dozen years since to err is human reminds us that as a whole the healthcare system hasn't taken on the challenge of monitoring, evaluating, and improving patient safety in a very aggressive and systematic way.

We're all hoping that health IT will be part of the solution to address safety, but we don't really have a denominator. We've talked a lot on the meaningful use process about indicators we think are desirable which we don't have a denominator. I would hope that the context in which recommendation one is offered is that the country as a whole needs to be monitoring patient safety and adverse event episodes

of which there may be a subset better attributed to HIT and its implementation in this sociotechnical environment.

Hopefully, we will help to reduce the incidence of patient safety issues and adverse events by implementing the technology, but to shine the light on the potential implications of HIT for patient safety without having a context that says on balance or on net, we may be having a very dramatic positive effect, but we're shining the spotlight on perhaps a relatively small incidence of adverse issues would be I think unproductive. It stimulates kind of a diverting debate. I hope one thing we can say to ONC and to the secretary is that the country as a whole should be aggressively monitoring patient safety and adverse event issues and looking for whether or not HIT is making a favorable impact on those.

Paul Egerman – eScription – CEO
I think those are excellent comments, especially what you articulated, the absence of a denominator. Those of us who have worked in this industry for years have seen tons of paper records where the information was just wrong or absent or multiple patients in the same record that didn't belong there. All of those things happen, and so the frustration is there is a lot of spotlight on this because it's the technology. Part of the reason why you have the spotlight on it is, well, first of all, it is an important issue. I don't want to minimize the issue, but anything with technology unfortunately gets this spotlight. I think that some people are enamored with technology and some people think all technology is just inherently bad. That's why you get that. I think the comments were excellent.

David Blumenthal – Department of HHS – National Coordinator for Health IT
Mike.

Mike Klag – Johns Hopkins Bloomberg School of Public Health – Dean
So, perhaps I could sort of respond to the question that David— So, were you implying that either in the goal or recommendation one to have a specific statement about reducing the incidence of adverse events?

David Lansky – Pacific Business Group on Health – President & CEO
I was almost pondering. In the goal statement, you could almost remove HIT from the goal statement and say we're supportive of patient safety, I don't have the language right in front of us, but patient safety improvements and understanding and monitoring the extent to which HIT is reducing patient safety or effecting patient safety outcomes.

Mike Klag – Johns Hopkins Bloomberg School of Public Health – Dean
I wanted to follow up on the first issue that Charles brought up about accreditation organizations. Paul, I heard you say that, yes; it's the intent of the committee that JCHO and other processes currently in place would be part of this. I read through the recommendations again and don't see it. You might want to just go back and see if you agree.

Paul Egerman – eScription – CEO
Let me see if I can find any for you. Just give me a minute. It's under a section called accreditations recommendations 6.0. Accreditation organizations such as the Joint Commission can play an important role in assuring HIT patient safety. ONC should discuss HIT patient safety concepts with these organizations to determine, for example, if they examine whether large institutions have patient safety review committees or where the processes are in place to encourage reporting—

Mike Klag – Johns Hopkins Bloomberg School of Public Health – Dean
… just didn't make it into a PowerPoint.

Paul Egerman – eScription – CEO
That's right, didn't make it a PowerPoint. Rightly or wrongly, I did that on purpose. I didn't think that I wanted to necessarily show a boatload of words on the screen, but it is in the letter.

Mike Klag – Johns Hopkins Bloomberg School of Public Health – Dean
Thanks.

Paul Egerman – eScription – CEO
Thank you whoever handed that to me. I wish all of life was like that. That was great.

Rick Chapman – Kindred Healthcare – Chief Administrative Officer/CIO/EVP
Rick Chapman with Kindred Healthcare. I just think we ought to maybe step back as a group, as I've listened to the dialogue and as a part of our committee I know we were guided by this, and reflect on that it is not the intent, and we were guided by this, not the intent of an information technology product in HIT to replace the intellectual processes of the professional and judgment of the professional via their license or the process itself, but you enable the three of those. This sociotechnical aspect you all keep talking about, all of us in information and health information technology for the last several decades have struggled with, but basically, it takes all three: systems, people, and processes. The process and the people (I agree with David, couldn't agree more) that in fact those two are the bigger role one might say and that the system can seek to enable and advise and present the opportunity for those people to act upon those processes to create the product and the outcomes that we want.

We need to be careful or else we need to get better direction from ONC. The scope of health information technology to achieve what we want is assumed to involve people and processes, but how far it's not the system. We could be making a mistake by going to the system saying that if we get the system to be perfect and regulated that it would somehow mandate or unusually effect people and processes. It can help. It cannot replace those intellectuals, and there are laws and rules and oversight of the people.

We should seek via our recommendations maybe to inform the processes, but I think it would be a mistake to put all of our direction just on the system itself and its defects, but just to seek to keep defect-free and then make them functional and if used correctly could get us to the outcomes. Again, I've made the oversimplification, but we seem to be doing such a good job of generating feedback that we tend to go outside of our primary focus I think from time to time, and I would just advise as a group that we keep within that IT focus.

David Blumenthal – Department of HHS – National Coordinator for Health IT
That's a very helpful comment and one that we should keep in mind. There are many organizations and agencies that have jurisdiction or for whom and for which patient safety is a central concern, HRQ, CMS, the FDA. There are many, many groups that have jurisdiction, and we have become one of them because we have a mandate to create an interoperable electronic health information system.

Information is such a protean and powerful component of the healthcare system that it's very hard to draw very strict boundaries, but your perspective, like the perspective I think of the committee, is a very apt one, that is that health information technology is embedded in a complex process, and its boundaries, one can extend our jurisdiction beyond where it ought to be. That's a balancing act we'll be constantly thinking about. We do have a responsibility to make sure that as we make recommendations that our recommendation's about the pace and manner in which electronic health systems are installed, does not stress those other systems that surround them in ways that are avoidable and that we interface with those other systems in a responsible way.

I think being aware of our boundaries but also being aware of the how important what we're doing is to everything else in that system I think are complementary perspectives. The perspectives need to be balanced, but I don't think there are any firm rules about it. I think it would be too narrow to address ourselves exclusively to technology because we have a broader mandate than just installing technology, but I don't think we can take responsibility for the entirety of the other systems, either. I realize that's not a definitive answer, but I think it's a matter of kind of judgment, but I also think that the committee's done an excellent job of pointing out those issues, the boundary issues, and David's comment extends … important one.

One of the questions that hasn't been discussed here explicitly is the issue of mandatory versus voluntary disclosure of reports and whether there is a problem with respect to inhibitions in the marketplace with respect to reporting. That needs to be addressed, in addition that relate to contractual arrangements between vendors and their customers. Did you come across any—?

Paul Egerman – eScription – CEO
It's an interesting issue. It's an issue we discussed briefly last meeting also, this concept of nondisclosure agreements and whether or not that prevents reporting. We actually did investigate that, and we couldn't find any evidence that those existed. We did find evidence that there are vendors who do not—we have contacts that allow the reporting, so there's choice in the marketplace, but we couldn't find examples of the vendors in the healthcare institution that signed contracts that would have prevented reporting.

Our view was rather than continuing to chase that issue, we just focused on what is the behavior we want to occur. You raise a good question about mandatory versus voluntary. The entire system that we have here is a voluntary system. People don't have to buy these systems. There's an incentive to encourage it, but they don't have to buy it.

What we tried to do in our recommendations was to say, well, if you want the incentive, though, you have to report. We created our recommendations in such a way that if these contractual restrictions exist, well, they're inconsistent with the incentive. People have a choice. Either they can go with the incentive in which they have to change their contractual … stick with that, their contractual … which they can't participate in the incentive. We think the incentive is incidentally a very powerful thing. That's how we approach the issue. We focused on the behavior that we wanted to encourage.

David Blumenthal – Department of HHS – National Coordinator for Health IT
Okay. David.

David Lansky – Pacific Business Group on Health – President & CEO
I have two specific questions of the certification workgroup I guess. Among the tools we have, obviously going forward are the certification process and the meaningful use criteria as we look out at the next couple rounds. I'm wondering whether with the discussion yesterday in the patient engagement hearing that Paul described about creating a more uniform mechanism for electronic health records to enable patients to download their data to an independent platform or whatever kind they wish and one could imagine in some future time much like we do with banking a very simple and commonly understood interface for downloading your data from a healthcare organization. At the same time someone made the comment that there should be an equally easy to use mechanism for correcting your data or informing the healthcare organization that there is something amiss as you described, Paul, that the patient can then give feedback to the organization.

I think if you look at the certification process going forward, it will be a worthwhile sidebar analysis. What would it take to work with the industry to evaluate some kind of uniform approach to that two-way communication with the patient where there is an opportunity to send corrections data back into the system and then propagate it however you need to propagate it. Given the HIE environment and so on, this issue of propagating corrections is going to be a challenging one, so it's something that I hope the committee will at some point think about.

The second issue is on the meaningful use side. Very early on in the meaningful use discussion a year ago we talked about adverse event detection and reporting. I think it would be worthwhile as we in the meaningful use process go back into this next round to take the perspective you guys have generated into are there meaningful use criteria that would give visibility to adverse events and the ability to detect them and reduce their incidence in meaningful use. It's something that providers could begin to capture and report.

Paul Egerman – eScription – CEO
Again, those are good comments. In one of our recommendations under recommendation two, we did very specifically say meaningful use should require patient safety reporting, and that's sort of like giving you a place to like hang your hat if that's the right expression to expand what that means. That could be taken in a lot of different directions, but that is one of the recommendations.

Stephen Ondra, M.D. – VA – Senior Policy Advisor
One of the questions I have about the correction of data is when you have multiple inputs to that correction. If there's disagreement about the correction, who's the final arbiter of what is indeed the accurate data?

David Blumenthal – Department of HHS – National Coordinator for Health IT
It sounds like we need a committee.

Paul Egerman – eScription – CEO
A big one. Ultimately, it's a good question, Steve, because as patients get more and more access to this, they're going to find a lot of issues with the data, some of which may not be clinically important. In other words, the patient may be very upset if the system says they weigh 165 pounds, and they really weigh 156 pounds, and people might think that's not important, but at the same time to the patient it might be very important. All I can say is it's going to be a very interesting issue.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Yes, I guess whoever owns the unique identifier for that particular patient. Just a jab.

David Blumenthal – Department of HHS – National Coordinator for Health IT
I'm going to take my chair hat off and put it on Paul's head to discuss the recommendations and their adoption or lack thereof.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
This is the point where we're going to decide whether we want to approve the letter as is or modify any of the recommendations. I don't know that I've heard a whole lot of corrections. We've heard some questions and then an answer that, yes, it's there. Does the group feel comfortable— yes, Christine?

Christine Bechtel – National Partnership for Women & Families – VP
… was absolutely right on on the first recommendation to list it on the broader context of patient safety. What I had was that we should aggressively monitor patient safety issues at large, including HIT's impact

on them or something like that. I think these are great, but I would strongly encourage us to include the spirit of David's recommendation on that.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
I think what you're suggesting is that perhaps we do go one by one. Any further discussion on that point? Judy.

Judy Faulkner – Epic Systems – Founder
The question of making sure that we've improved in patient safety brings up compared to what. If it is has the electronic health record improved, then you have to say, what if they didn't collect data before they installed, or what we find frequently is even though they intend to, they don't. I think that we have to keep that in mind. Are we counting year-to-year improvement using the system or before when they were paper and how does it compare?

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Can I ask one question of both David and Christine then? If we take out the explicit or reference to HIT, would we be asking this independent organization then, for example, to study patient safety at large? Paul did mention the Institute of Medicine, and clearly, they had a series on quality matters in patient safety. Are we asking for a restudy of that, or is it just a slight change in the words to say what's the role or impact on positive and unintended in patient safety?

David Lansky – Pacific Business Group on Health – President & CEO
I think we have a distinct responsibility to address the HIT implications of patient safety … HIT, so I don't want to dilute that. At the same time, I'd like as Christine said to alter the high-level language here and maybe some of the sub-bullets to indicate that we want HIT to be used to monitor and improve patient safety broadly. This is not a strategy to just look for the flaws of HIT, but to, as Judy says … of HIT can allow us to capture information about current practices, patient safety implications and to assess any positive or negative effects introduced by HIT.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Okay, so not lose the focus on HIT, but perhaps reword it a bit to understand its role in patient safety both in assessing it, in improving it and watching out for unintended consequences, something like that. Is that fair, Christine? Okay.

Should we go ahead and vote on that piece then, recommendation 1 and 1.1? All in favor? Are there any opposed and any abstention? Okay.

Let me ask maybe globally are there any others that we want to pull out for separate discussions? By the way, following the PowerPoint is the actual text of the letter, in case you're looking for that. Yes, Christine.

Christine Bechtel – National Partnership for Women & Families – VP
I have a question that I think is really for Paul and Marc, which is on recommendation two. Copies of those reports should be sent to any vendors that might be involved. Should that really be all vendors or is that too much?

Paul Egerman – eScription – CEO
What do you mean by all vendors?

Christine Bechtel – National Partnership for Women & Families – VP

It says copies of those reports should be sent to any vendors that might be involved. If we're sending reports of patient safety issues related to HIT, should they just go to the vendor whose system was involved, or should they really be broader and go to everybody in the vendor community so that they're aware of the potential.

Paul Egerman – eScription – CEO
What we had intended with this was this is the notification from the healthcare organization to the patient safety group as to what they think is a problem. We said any vendors involved. We specifically meant that to be the two or three vendors that they think were involved with this that they be informed that their notification was going on. The issue of sending information to all vendors, that would come from the patient safety organization … doing the oversight, but that doesn't come from the healthcare organization. That's now their challenge. Their challenge is just to … their vendors.

Christine Bechtel – National Partnership for Women & Families – VP
We're saying the same thing.

Paul Egerman – eScription – CEO
Yes, that's right.

Christine Bechtel – National Partnership for Women & Families – VP
That was … this, but we're saying the same thing.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
It causes another question, though. As you know a vendor may have let's say databases baked into the shipped product, and it may be in fact be that database that causes the error or provokes the error. Is the customer responsible for knowing all those subcontracts or subparts of the product, or do you just report to the vendor who you purchased the product from?

Paul Egerman – eScription – CEO
It's a great question, but at this level reporting, first of all, I think the healthcare organization probably is in the best position to figure out which are the vendors that are involved. This process will eventually have a lot more refinement where the vendors can respond, and they can say it's not really my thing. It's this other guy's database problem or it's this other operating system, and they can clarify it later. This is just to start the process going. It's not an obligation for the healthcare organization to try to go through that, although my expectation is, say next to Marc, that somebody like Marc would be submitting something actually would probably be very helpful in terms of being able to say these are the three or four vendors who might be involved in the situation if you want to comment on that at all.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Well, I think that if I purchased a product from a vendor, they're going to understand who their third parties are that they're involved with, but I would want to contact the vendor of let's say the EMR system, maybe the lab system. I'd probably go to someone like Cisco if they're the people that are working on my networks and I thought that had something valid. Neither of those first vendors would have information about it. It is pretty complex, Paul, actually.

Any other comments on recommendation two? Okay, all in favor? Any opposed or abstained? Good. Anyone want to talk about recommendation three? Four? Five? Six? Seven? Mike?

Mike Klag – Johns Hopkins Bloomberg School of Public Health – Dean
Do you want to put a specific days in rather than …? Do you want to put the calendar date?

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
How do you feel about that, Paul and Marc? I know Judy raised the question that 18 can't automatically apply to everything, but you've got to start somewhere I guess. I think that was … in the ground.

David Blumenthal – Department of HHS – National Coordinator for Health IT
I'm going to advise my colleague, Tony Trenkle, to comment on this only because we are in the midst of rule making, and the rule is not yet finished. So, putting dates in the sand would have implications for that.

Tony Trenkle – CMS – Director of OESS
I'd agree. One of my concerns here is the fact that we want to get some feedback from the different phases of the program, particularly the first year as we begin to roll this out. Although this sounds on paper like a good requirement, if you start backing up the dates, it really wouldn't give us a whole lot of time if any to get any feedback on the 2011 responses and some of the concerns that come up. So that would be my major issue with it, at least for stage one as we begin to roll out the program.

Stephen Ondra, M.D. – VA – Senior Policy Advisor
The other problem is, though, we end up passing the buck to somebody who's got to implement it at the backend if we don't get some solid lead way into getting requirements out.

Tony Trenkle – CMS – Director of OESS
It's certainly a balancing act. I think it would have the effect of probably slowing down some of the stages to some extent because of that.

Stephen Ondra, M.D. – VA – Senior Policy Advisor
Not to defend the recommendation, this recommendation would work. It's just 18 months before that stage is required.

Tony Trenkle – CMS – Director of OESS
No, I understand. I'm just saying if the intent is to move to different stages at different time periods, this would have an effect to slow down those stages, and that may be what people want, but that's—

Paul Egerman – eScription – CEO
I'm confused. Do we have the ability to slow down the stages?

Tony Trenkle – CMS – Director of OESS
There's nothing … about the stages. The stages were in the NPRM.

Paul Egerman – eScription – CEO
So we could stick this the way it's said. In other words, we stick with 18 months before the eligibility period, which means that we would change the eligibility period for stage 2 instead of October 1, 2012.

Tony Trenkle – CMS – Director of OESS
Right, you could potentially do that. As I said, the stages aren't statute. The idea of stages was put out in the NPRM. It was recommended, of course, within the policy committee as well, so that obviously can be changed and the final rule can be changed and subsequent rule making.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO

Eighteen months can certainly be part of the recommendation. The word finalize does have very definite meanings, let's say, to a CMS rule making body. One of the ways that we in the policy committee have been trying to deal with this issue about the … wanting to get some feedback, but yet give the market a chance and the providers a chance to react is to try to go into signaling mode, which is not the same thing as finalize. Do you see what I'm saying? There may some flexibility on how we work together on that tension in the timeline, but finalizes wouldn't allow us to do that and effectively carry out this recommendation. Does that make sense?

Paul Egerman – eScription – CEO
It does.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Do we really want to finalize?

Tony Trenkle – CMS – Director of OESS
Maybe you want to change that word?

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Yes, that's—

Paul Egerman – eScription – CEO
Judy, do you have … the vendor representative.

Judy Faulkner – Epic Systems – Founder
I think in the discussion in general we were thinking of patient safety. This is a very much broader thing than patient safety, and that's why I think Tony's comment and others are very valid. It's kind of scary to have such a strong ….

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Again, if we go back to either what David said, we're here about patient safety, not implementing these things because of a word could be devastating if not more so. There was a reason why there were dates picked. There's a reason we have waited this long as a country, but we've just go to get on with it. What can we do to get on with it and address all the valid needs that all the stakeholders have? Is finalize getting in way? Could we be writing something that gets in the way of that?

Tony Trenkle – CMS – Director of OESS
….

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
That's correct.

Tony Trenkle – CMS – Director of OESS
… choose to go with or not.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
We're trying to be as precise as we can be, and this group has been very deliberative and tried to be very precise, and so we're just trying to do as right a thing as we can do knowing that we're only advisory.

Tony Trenkle – CMS – Director of OESS

The concept of patient safety does come through in this recommendation, that things are done so hastily that on the receiving end of this, the actual implementation side of this that it can be done in a well thought through and safe manner. I think that was part of the issue driving. The sooner we can get the requirements out there, they can be reacted to. I understand the concern with finalized and something like provided—

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Or maybe known.

Tony Trenkle – CMS – Director of OESS
Or known.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Because instead of finalized, they're known. Instead of having ….

Tony Trenkle – CMS – Director of OESS
Available and provided something.

Paul Tang - Palo Alto Medical Foundation - Internist, VP & CMIO
Why don't we give ourselves a couple choices? How many prefer available? I'll have to count, as opposed to finalized, finalized versus available. It would be appropriate to just say the recommendation would then say available, right? There are a lot of words we might prefer, but can we go with that? Can people live with something like available and not finalized? Let's do a little bit … because we might have some … in disagreement, opposed, okay, good. We have rewritten seven.

We're now up to eight and nine. That would ensure that we still have a job. With the exception of the amendment to seven, then all in favor of approving the rest of these ones that we hadn't voted previously on and any opposed. Motion carries and we have essentially another approved letter to the National Coordinator.

David Blumenthal – Department of HHS – National Coordinator for Health IT
Gratefully received. We are at break time. Yes, Judy, do you want to say something? That was like an alert. We have now a decent interval for lunch. Reconvene at 12:30 and appreciate your attention and sorry about the weather if you were thinking about going outside the hotel. It could be worse. It has been worse and could be worse. Anyway, thanks very much. Thanks again to the committee for their recommendations.

Judy Sparrow – Office of the National Coordinator – Executive Director
If everybody could please take your seats, we're ready to begin the meeting. Dr. Blumenthal.

David Blumenthal – Department of HHS – National Coordinator for Health IT
I hope those of you who are still eating lunch can eat lunch and listen at the same time. Those of you who have to speak may have more trouble, but anyway, we want to welcome our next report from the privacy and security policy workgroup, Deven McGraw and I don't know if Rachel is on the phone, great. Welcome, Rachel. I saw her in New York yesterday.

Deven McGraw – Center for Democracy & Technology – Director
I think I'll do this from here unless folks have objections to that and want me to sit in the pit.

David Blumenthal – Department of HHS – National Coordinator for Health IT

No, that's fine, anywhere you want, Deven.

Deven McGraw – Center for Democracy & Technology – Director
We have a few slides here. There are not very many, but what we want to do mainly today is to use this as an opportunity to update the committee about some of the issues that we've been discussing over the last month, say month and a half, and get some preliminary feedback.

What we've been focusing on is privacy protections for electronic health information exchange, including but not necessarily limited to what is the role of consumer choice or consent in a framework of privacy protections that ought to apply to electronic health information exchange. We're not presenting specific recommendations today, and I really want to underscore that because even though we do have some slides with some language on it, we did that so that you would get an understanding of sort of the direction we're heading in so we could get feedback from you. We want to have a sort of complete set of recommendations ready for the main meeting, but we thought it was worthwhile to let you know again what we're thinking about and consistent, David, with something you said when we were first chartered, which is to say give the committee a little time to digest and give feedback on some of this stuff before we finalize it, and so this is a little bit of a sneak preview of what may be coming, but in fact, there's still a fair amount of work yet to be done on the set of issues that we're going to talk about today.

We start with the principle, of course, and it's always worth repeating that privacy and security are foundational to achieving meaningful use of health IT and that a comprehensive set of privacy and security protections that build on current law and more specifically implement principles in the nationwide privacy and security framework is critical to building the foundation of trust that will support and enable meaningful use by providers, hospitals, as well as consumers and patients. There are sort of two things in here that are worth drawing out. One is we're building on current law. We're not working from scratch here. It's not like we don't actually have some provisions that are already in place. At the federal level, that's largely HIPAA, but also includes the protections on substance abuse treatment records under part two and of course state law, which plays a very important role here.

The nationwide privacy and security framework is a principles document that was adopted by the Office of the National Coordinator in December of 2008, and it's largely based on fair information practices which are the sort of common vehicle for defining privacy protections of personal information in all sorts of contexts. Again, we use that not as though those are written in stone in part because they're principles, but to sort of serve as a guide post for coming up with a more detailed implementation regulations. I think we've mentioned the framework in the context of the strategic working group as well, and so it's a document that's very helpful for fleshing out details, but the important message I want to convey here is that those are really just a starting point and that there needs to be a lot more detail in order to build essentially the trust framework that will enable health information exchange.

The next bullet, and this is quite consistent with not exactly recommendations, but the update we're going to get from the NHIN workgroup later on today, which is to say that health information exchange to meet meaningful use is likely to take place in a number of ways. What's needed to build and maintain public trust may vary depending on how the exchange occurs. For example, if it's one-to-one exchange among providers such as using NHIN Direct, as we sort of scope that out, what's the trust framework that needs to be in place for that versus what may need to be in place for a health information organization, the sort of … entity that's being created by a number of states to help facilitate exchange in those areas. All along as a committee we've talked about how, and we've done this in the IE workgroup as well that exchange, there's likely to be a number of different models through which this can take place and essentially recognizing that we need to build trust in each and every one of them, but it might take different components to hit that depending on what's involved.

In our approach to this question, one key theme has been coming up over and over again, and that is what are the reasonable expectations of consumers and patients with respect to exchange and how their data is shared and for what purposes and with whom. And while that's a sort of foundational concept that has come up a lot in our discussions, we also, of course, recognize that in fact some patients may not be aware at all about what happens to their data and others are a bit more sophisticated, but where I think at its basic level what we're talking about is when data is exchanged among providers for treatment purposes where the patient knows the provider, trusts the provider, and may in fact know in many cases the provider to whom the data is being sent, disclosed to, for example, in a referral relationship or understand that some data needs to be sent to a health plan in order to check eligibility.

In essence, that concept where, again, it provides a jumping off point for the discussion, to what extent are these new vehicles that we are creating for exchange or the processes and procedures and standards that we're putting in place to ensure that exchange occurs? To what extent are these deviating, for example, from what patients either expect in general or what's essentially reasonable, within reasonable expectations?

We've sort of in the workgroup gotten largely comfortable, and again, we want your feedback on this, with one particular type of exchange or one could consider it to be one end of a spectra of types of exchange. That is what we're calling one-to-one exchange where you have an eligible provider, and this is picking right up on the meaningful use language, or a hospital who's engaging in one-to-one exchange in order to meet the stage one criteria for meaningful use in accordance with the NPRM, no additional individual consent or authorization requirements should be imposed beyond those that would otherwise apply under state or federal law.

Number one, we're talking about no additional consent requirements. It doesn't mean we're overriding those that already exist in law, whether that's at the federal level or state level or, of course, an institutions voluntary policy to seek patient consent in certain circumstances. They can in essence still do that, but we're talking about not imposing additional requirements.

We're also talking about the exchange functions that take place to meet the stage one criteria of meaningful use, which is very much focused on treatment and reporting for public health mandates. Some quality reporting, of course, to CMS, but the assumption is that in most cases that's going to involve aggregate data. It may or may not be de-identified data per the HIPAA standard, but it's aggregate data. Again, much of it when it's involving exchange directly with patients, where the data's being sent to patients, one assumes that the patient has in fact consented to receive that data and that the data is going to the place. For example, if the individual wants it sent to a PHR, then it's going to that patient's choice of a PHR if in fact that happens.

It also assumes that if there's an "intermediary," and the term intermediary is in quotes in part because the definitions around some of these terms have yet to be universally accepted. So essentially, if there is an entity in the middle that's facilitating the exchange on a one-to-one basis, so essentially if I were a primary care doctor and I wanted to send information to a specialist, somebody might have to help me make sure that electronically it got from my file to the referring provider's file in order to facilitate care management or further treatment of the patient.

The intermediary question and how much access to data that intermediary has and what they can do with it is the more open issue that the workgroup is still grappling with. If in fact the intermediary, maybe it's a vendor essentially that sends it from one point to the other that the access to data is limited to what's necessary to send it from point A to point B and they don't necessarily store it or retain it or use it for any

other purpose. In general in the context of our conversations, folks have been largely comfortable that we likely don't need additional patient consent requirements to layer on top of that, although I think you would still need policies about how any data that might be accessed by an intermediary in order to facilitate that transport would be managed just as should be the case with anyone who essentially touches and handles data.

Part of the reason why we're reaching a level of comfort with this is because it's in fact in many ways arguably digitizing the data sharing environment to the extent that it exists at all that exists today, which is essentially with the provider sending or authorizing the sending from his or her electronic record to another provider where the trust relationship between the provider and the patient in part should create a level of comfort with respect to the patient because essentially it is that patient's trusted provider with whom he or she has a treatment relationship who is essentially the arbiter of the data flow. But, again, we are also talking about being comfortable with this in the context of stage one of meaningful use, which is not an unlimited set of access, use, and disclosure of data.

Now we get to a place where we are continuing to deliberate and where we are hopeful to have recommendations by May that we would present in conjunction with the one-to-one exchange recommendation assuming after we get through all this we still maintain our level of comfort with it. That is what about the intermediaries in the middle, and what set of policies ought to govern their access to data, and at what point does it reach the point of not being within the sort of realm of reasonable consumer expectations where we would want to give patients some choice about whether or not their data can be accessed through or deposited into, depending on the structure, the intermediary. I think this is a tough question that we would very much like to get some feedback from the workgroup.

One document that has at least been helpful to me in trying to think through these issues is a white paper on consent that the Office of the National Coordinator had commissioned. It's not a short read, but I think it's a very thoughtful read, and it takes a look at what the different states have done on the issue of consent. To me what makes it interesting is, one, is that there are a lot of different models out there that they're using and that the consent piece is just one of many protections and sets of rules and policies that built in to the exchange network in order to build trust.

For example, they have all made decisions about the purposes for which that state exchange can be used, and most have limited it in some way—treatment, public health, some research functionality, but there are some clear policies that have been set forth about the way that the exchange can be used, similarly, who has access to data through the exchange and what are the sort of security policies and standards that are used with respect to the exchange of data. It's a very complex picture of the way that you can build trust and in exchange using sort of an intermediary that may be playing a more robust role than a simple moving from point A to point B and creates I think some interesting challenges for us as a workgroup given that we're not stumbling onto this issue before people have started to lay some groundwork and that any recommendation that we provide I think will need to be very sensitive to the potentially disruptive effect it might have on existing entities, albeit maybe it's a disruption that might be needed. That is, of course, something to decide.

The other issue here is what I'll call loosely, I phrased it here as build on HIPAA business associate provisions, but it's actually a bigger question which is what are the tools that ONC has to essentially impose a set of trust framework requirements or suggestions, recommendations on the intermediaries that are going to facilitate these transactions. One vehicle is of course through grant conditions to states, but the other potential vehicle which has the opportunity for broader reach, but isn't fully within ONC's control is through the business associate rules under HIPAA. For those of you who aren't as familiar with what a business associate is, essentially, if you are receiving protected health information from a covered

entity in order to perform a function on that entity's behalf, you have to sign a business associate agreement and your uses of the data are limited to the terms of that agreement. In the high-tech provisions of the Recovery Act, Congress said that RHIOs and exchange-type entities should be business associates, so essentially, that provides potentially a framework in which to think about sort of additional requirements that one might impose on intermediaries who have data in the middle.

But it's also not without its complications because in the past those agreements have largely been for the covered entities to decide the content of them. They're limited. They can't authorize the use of data beyond what HIPAA may require, but they're still pretty open with respect to what those are required.

I think there are a number of challenges that we could and I guess I would argue should potentially address. One is what are the sort elements of the trust framework that we want to put in place, and how specific do we want to be. At what point do those higher levels of requirements or recommendations get triggered? What are the functions and features of an intermediary that goes beyond just what's needed to facilitate the transport and where it starts to have access to more data for a variety of purposes where we would want to, number one, put some maybe more specific requirements on how data can be used and who can access it and for what purpose, sort of basic elements of fair information practices as well as allowing consumers a voice in the process, i.e. I get what this is based on, but I'm still not comfortable with my data being accessed through it, and I ought to have some choice about that.

We are trying to grapple with that and feedback would be most welcome. I'm going to stop and ask my co-chair, Rachel, if I have messed anything up or if she wants to add anything, and then I'll ask members of the workgroup to make sure I'm being honest about our deliberations, and then I think we should open it up to the rest of the committee.

Rachel Block – New York eHealth Collaborative – Executive Director
No, thanks, Deven. This is Rachel Block. As always you did a terrific job of summarizing. I have nothing to add.

Deven McGraw – Center for Democracy & Technology – Director
Anyone from the workgroup want to chime in, make sure I characterized this right? These have not been easy discussions, but I have to put a plug in for my group working very hard. We're having basically full attendance on every call, and it's been extremely interesting. I know I'm learning a lot. I'm not sure how much progress we're getting to a consensus, but we'll get there. Gayle.

Gayle Harrell – Florida – Former State Legislator
I'll make a few comments. As part of this workgroup, I think this is one of the most important things we're doing, privacy and security and building that trust that's necessary in order for patients, and we always as we had this conversation this morning, we want to look at everything from the patient perspective, and that's really the core of what we need to be doing, developing. This is not an easy job in determining how we're going to go about it. I don't know that we've come to any real good answers at this point. To me, we're moving along. We're making some progress.

I think the idea of a trust framework is very critical, and I was pleased to see that I guess that David's group is working on that very well. I think people need to understand that once we come to some conclusions this is going to take a major public relations endeavor. People need to understand what that trust framework really is. Consent is a very important part of this whole thing as well. I think making determinations how you do that is difficult, but one of the basic things that's going to have to come out of this committee is what patients have, what consent is, how they can control their data. That's absolutely

critical, so I'm enjoying being part of that group, and Deven does an outstanding job in keeping us all in line.

David Blumenthal – Department of HHS – National Coordinator for Health IT
Thank you to Deven and Rachel and thanks to the group for this initial report. The focus is on exchange and on the context for exchange. I gather that's sort of the organizing framework you're using and that your recommendations on consent will be contextualized to the kinds of exchange that are taking place with respect to patient data. Those the branch points you're going to be using?

Deven McGraw – Center for Democracy & Technology – Director
Yes, it's really very difficult to think about consent outside of the context because then the question, consent to what. What are we asking people to consent into or out of? What are we putting in front of them? I think we have a responsibility to set that frame as much as we have a responsibility to consider the parameters of choice.

David Blumenthal – Department of HHS – National Coordinator for Health IT
Yes, Charles.

Charles Kennedy – WellPoint – VP for Health IT
… the notion of patient control and empowerment, and I'll relate it with a story we had in one of our e-Prescribing pilots. We had a patient who had two treating physicians, an internist and a psychiatrist, and as part of e-Prescribing, you can download a patient history from claim data that comes from both physicians. Anyway, she had never told her internist that she had a psychiatrist. She was quite upset and felt that her privacy had been violated. I say that to mean that under HIPAA we may be able to meet the criteria and share data because both physicians had a treatment relationship, we may not be truly respecting the patient's intent.

The other point I had was the physician, the drug that was shared was lithium, and so any physician would have a very good idea just based on that alone. There was no diagnostic information shared. Just blocking out the diagnosis without the correlating medicine is probably not sufficient privacy either.

David Blumenthal – Department of HHS – National Coordinator for Health IT
Yes, Neil.

Neil Calman – Institute for Family Health – President & Cofounder
I think one of the critical things we need to think about is as these exchange models develop and if they're regional, patients probably won't have much of a choice. The idea that you're either going to opt in or opt out, but don't really have a choice maybe in your geographic area or in your network or whatever of whether or not there are different models of exchanging and whether or not particular entities are more trusted than others. I think we're going to sort of be in a position that's unlike what most consumers get to do, which is to sort of pick the people who they trust to do business with. We may not really have multiple choices in various areas, and I think we have to really think about that because the idea of forcing somebody to either say, well, you either work with this entity. Yes, we know they've had some problems and there's been some stuff in the papers and whatever, or you just don't get to exchange your data, which we all think is a critically important thing in relationship to value in healthcare. It's probably not the endpoint that we want to reach, so that's just another thought. We have to figure out how we're going to deal with that issue.

Deven McGraw – Center for Democracy & Technology – Director

I've also often thought that if people are at the point where they have so little trust in the system that they want to opt out of it or fail to opt in, we haven't given them very many options. It almost feels like a failure in some way that if we can't structure a system that does better by patients so that most of them have some degree of comfort in it. There are many times when it feels like opt out or failure to opt in is I would hope that would be the last resort. We could do better to structure more trust and more care about who has access to data and for what purposes, and then people wouldn't feel compelled not to. There still probably would be some folks for whom we couldn't reach that level of assurance, and we have to think about arguable creating a system that works for all of those patients if we can.

David Blumenthal – Department of HHS – National Coordinator for Health IT
Yes, Tanya.

Latanya Sweeney – Laboratory for International Data Privacy – Director
I've said it before. I'll say it again. I still think that the intermediary infrastructure could be lightweight. It could be onerous, and you just don't know what it is. One of the problems with sort of over-fitting the thinking to one-on-one is one-on-one is only going to get you so far until that's not what the model is. Even in the one-on-one model, you still don't know what the infrastructure is that allowed the two to connect to one another or how much that model required, what kind of data sharing it required in order to be operational.

I think expectations are fine, but overall, you need a model for a social maximal utility. You're going to have to figure out from the overall structure what are the real harms because any design of the infrastructure is going to introduce new harms that could not have been predicted by HIPAA. To say that, well, it's okay because we're still sharing under HIPAA is like sort of blinding your eye to the sort of model. If you took the model I don't want to do any more harm than what's already happening, I think that's a good model to think about in terms of these infrastructures.

David Blumenthal – Department of HHS – National Coordinator for Health IT
Paul.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Yesterday I talked about elephants, so I'm not going to go quite there, but the concept if there's some overriding either authority or model, in yesterday's case it was the reimbursement system, does it take a thousand other ways to compensate for that to correct that. In this case maybe the question is do we need to figure out all the different ways to permit people to do something, or is an alternative approach to hold everybody accountable. In a sense, one of the loopholes in HIPAA is we only have the three covered entities. I don't want to suggest anything, but is the accountability the problem, or is it a permission problem, which is the root cause and which could be more potent in fixing.

Rachel Block – New York eHealth Collaborative – Executive Director
This is Rachel Block. I think just based on our experience here in New York I would say it's really difficult to say it's one or the other. I think it is a balance, and we certainly did a similar analysis in terms of sort of roles and responsibilities and risks and benefits as we were driving towards consensus on our policy which, again, is something that worked for us and may or may not be appropriate for all settings at this point. I think I would say that it's almost impossible to choose between those things. You might decide to weight them a little bit differently based on some of those contextual factors that Deven described.

Deven McGraw – Center for Democracy & Technology – Director

If we think the set of rules that we already have don't appropriately address the risks we know of today much less those we can't anticipate tomorrow, just expanding them to cover a broader universe doesn't necessarily address the problem, but I think there are dimensions of both.

David Blumenthal – Department of HHS – National Coordinator for Health IT
Mike.

Mike Klag – Johns Hopkins Bloomberg School of Public Health – Dean
Just a reaction to what Latanya said. My impression of our discussions in the workgroup was not that we're punting and that we're satisfied with the status quo. It was that we have a foundation, and then we will critically examine what new needs they are, but to build on that foundation. I think it's a different interpretation than what you took from Deven's presentation. What is the impression of the workgroup …?

Deven McGraw – Center for Democracy & Technology – Director
I would actually like Latanya to address this, but what we have been saying with respect to one-to-one exchange is that because it's largely consistent with what happens today in paper form to the extent it happens at all, we don't see that there is a need, again, sort of almost based on the reasonable consumer expectation theory, for additional consent or authorization requirements beyond what's in HIPAA. Of course, I think Latanya rightly points out that it's limited in many ways because it looks at what types of exchange are called for under the stage one meaningful use criteria. We haven't sort of gone beyond that, and it assumes a very basic exchange model that may exist initially in the initial years of this grand experiment but may not last for very long as things sort of get more sophisticated.

Latanya, were you specifically saying that you didn't like the recommendation one because there are some shortcomings in HIPAA that you think we need to address where consent would be one way of addressing them? Or was it more that it's a quite limited recommendation because its scope is so narrow and it might not stand the test of time?

Latanya Sweeney – Laboratory for International Data Privacy – Director
I think its scope is maybe even orthogonal to the way reality may hit. Let me give you a good example. There is an assumption made that one-to-one, when I move it into the technology space, is going to be the same as it is now. Fax is the current way it's done now, right? Suppose I'm maliciously trying to find someone, and suppose the one-to-one is very lightweight, and it's lightweight in that we're all given particular kinds of email addresses or kinds of identifiers if you're in the club. If you're not in the club, you don't have one of those, but being in the club, there's still a really large number of people. If I was a domestic violent stalker or just being malicious, I could actually ping every provider in that network to find the patient I'm looking for, but you can't do that by fax because if I call up an office and say, "Well, look, I'm looking for David's information," I've got to convince them, one, that I'm legitimate and they sort of informally … whether or not it's worth their time to fax something. Does this really need to go? That poses some really natural barriers that the technology, even a lightweight technology just totally tore down.

Deven McGraw – Center for Democracy & Technology – Director
That's actually the scenario that we in the workgroup have categorized as more robust intermediary for which we do think there needs to be more. The query response—

Latanya Sweeney – Laboratory for International Data Privacy – Director

It's not a query response, just the email. Not even a query response. This is just only email communication where a human is going to interpret the email. The point is I can't make 1,000 phone calls, but I could send 1,000 email messages looking for David's record.

Deven McGraw – Center for Democracy & Technology – Director
Right, but David's doctor is the only person who can release that record.

Latanya Sweeney – Laboratory for International Data Privacy – Director
Right, but I don't know who David's doctor is. I want to know whether or not David is a patient. I send an email query, and so then the other flip side of it, that was the lightweight one. Look at what an onerous one looks like. An onerous looks like a very detailed master patient index in that community. That creates another set of privacy issues that are also orthogonal to that perspective even thought the communication is one-to-one.

Deven McGraw – Center for Democracy & Technology – Director
I think you are exactly raising some of the sort of this determining what functions and features trigger a more robust set of requirements. I think we have assumed that in the scenario that you just laid out, in the email where you're looking for David's doctor, you don't know who David's doctor is, that if David's doctor responds to your email that David's doctor isn't going to just send you data without some indication of why you're asking.

So in many ways, part of what makes many of us comfortable with one-to-one, I don't want to say all of us again, these are not final recommendations, but for the most part we've been largely comfortable because it still will take the data steward, David's doctor, deciding, yes, this person has a legitimate need for this information, the person's treating physician, and I will push that data out per person's request, because I think it's—

So in other words, David's doctor almost acts like a proxy for David in terms of consent. It doesn't mean that we wouldn't layer some and we should I think layer some very specific protections on that, but we sort of came at this set of questions initially through the consent pinhole and we're trying now to sort of contextualized that in a little bit, in a way. But I think you're raising some important issues.

Latanya Sweeney – Laboratory for International Data Privacy – Director
I would just say that the answer that you just gave doesn't mean one-on-one. It means that someone vetted. That might have even been technology to do the vetting, which is a totally different model and has nothing to do with one-to-one.

Deven McGraw – Center for Democracy & Technology - Director
Right.

Latanya Sweeney – Laboratory for International Data Privacy – Director
Or one-on-one, right?

W
....

Judy Faulkner – Epic Systems – Founder
… HIE either. It's a whole different thing, and I mean right now anybody can e-mail a lot of people and say which doctor is taking care of this patient that's not an HIE subject I think.

Latanya Sweeney – Laboratory for International Data Privacy – Director
But I think she was trying to model the fax and she saying we're not doing any more harm than the main way it's done, it's just faxed. And then my point was, well actually technology changes even something that simple.

Deven McGraw – Center for Democracy & Technology - Director
Yes. It's a very good point, that the provider has had an opportunity to vet that and make the ultimate decision about the release of the data, I think it's one, and so I'm collecting the functions and features that trigger.

Latanya Sweeney – Laboratory for International Data Privacy – Director
But with that, I just want to say that the fact that some of this is vetting is not the same as one-to-one communications. It was the fact that I said I'm sending e-mail and somebody had to respond to e-mail that brought up a vetting issue, but that vetting could have also been done by technology through some kind of authentication systemic. There are lots of other ways it could have been done. It seems like the value is on the vetting.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
David?

David Blumenthal – Department of HHS – National Coordinator for Health IT
I just had a really small point. On this slide, I was just thinking that the accountability oversight tag doesn't explicitly call out redrafts. And in terms of this consumer confidence issue, I think that will be an important thing to make very visible for the consumers that they have a channel, given this issue, the scenarios you described around levels of trust or Neil did with different entities, maybe bring that out more visibly.

Deven McGraw – Center for Democracy & Technology - Director
Good point.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Yes, Art.

Art Davidson – Public Health Informatics at Denver Public Health - Director
Yes, I'd like to go back to the example that Charles gave of the e-prescribing, because I'm not sure that we have really come to any conclusion about that. And what the policy committee should be thinking about with regard to splicing and dicing permission to specific data versus not, and the potential risk and adverse events that could happen if they're not exposed to that. I don't know whether the workgroup has really thought that through.

As you say, each state seems to have found a way to solve the issues of consent, and in my state, it was global. It's either you get it or not. But with the emphasis on e-prescribing in stage one, it seems like we're being forced to engage with Surescripts, and I don't know that Surescripts is ready to say, I understand how you spliced and diced, and this Lithium is off limits to this doctor. And I don't know how we're going to address that.

Deven McGraw – Center for Democracy & Technology - Director
Well I don't want to say that we're not. I mean we did early on as a workgroup say that we would attempt to try to address this issue in a broader context first and then drill down to sort of more narrow context

about types of data. And then we got into the discussion of what's broad. Does that mean all in or all out or choice by type of provider? Is that still sufficiently broad?

And we may, our next call is on Monday, and we may get into this discussion again, because it's very hard to keep the discussion separate because one obviously has an impact on the other. We are going to get to the issue of that level of granularity where it's down to the specific type of data, and the medication data is the one that's really difficult because and I think you all have presented the issues very squarely. The patient was very upset that that got shared without her consent, and yet the psychiatric drugs are among the most reactive with other compounds and if there isn't an ability to know that, it could have consequences. Do you allow the patient if they understand those consequences, is it their job to live with it, and how then do you scale that to a set of policies that are going apply across all patients. So I think it's hard. We have not gone there, we intend to. If you want to join our calls, let me know.

David Blumenthal – Department of HHS – National Coordinator for Health IT
I was trying to make that point and thought it was important of the patient empowerment piece, because many of these systems that are designed today, the patient is kind of not in the middle of that. Surescripts, there's no patient portal to and I was just trying to highlight Gayle and Deven's point, that that's something we need to address I think much sooner than potentially we even think.

Art Davidson – Public Health Informatics at Denver Public Health - Director
It's actually part of the R8.

Deven McGraw – Center for Democracy & Technology - Director
Yes.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Yes. Mike?

Mike Klag – John Hopkins Bloomberg School of Public Health – Dean
So as a physician I wonder whether that's even within our purview, because that is a great issue, it's a great example. Because not only is it adverse drug reactions, which you were referring to, but the side effects of Lithium cause a variety of metabolic dysfunctions. It's absolutely essential for the internist taking care of that patient to know they're on Lithium. So you get into issues, I'm not sure that this committee can get that granular. In fact, I would argue strongly, we can't get that granular.

Deven McGraw – Center for Democracy & Technology - Director
Although it's hard, because we are trying to set policies that will enable exchange and knowing that's just a very type data. I will say that I hear, and this maybe actually in the consent paper, that many states are deciding that the way to weigh, and this doesn't apply e-prescribing per se, but many states are saying that the way to avoid dealing with the issues, particularly around the sensitivity of mental health data, is we just won't include it. Which means it's not part of the data that's available. And of course—

Mike Klag – John Hopkins Bloomberg School of Public Health – Dean
And so then that counters our goal about patient safety. That is absolutely contradictory to the patient safety.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
So we'll need to wrap this pretty soon. Is there any other comments of the group or comments to feedback into the work place? Well they're laboring hard and intensively on trying to at least address these issues that we have to, but they're still hard. Always have been for decades.

Our next workgroup, thank you very much Deven and Rachel and the workgroup. The next workgroup is the NHIN workgroup to talk further about their trust framework, and that's David and—

David Lansky – Pacific Business Group on Health – President & CEO
I want to make a scheduling adjustment. Tony and I might swap places.

Tony Trenkle – CMS – Director of OESS
We're going to swap places.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Absolutely. Tony? Wherever you're comfortable.

Tony Trenkle – CMS – Director of OESS
Okay, so I'm going to give everybody a latest and greatest status here on the regulation. As I spoke last month, we talked about some of the initial work that had just been kind of getting underway, because the comment period ended on March 15th, and we had a meeting shortly around that time.

We have now finished cataloging the several thousand comments that were received. We begun the process. We have drafted the reg, it's been drafted in pieces, and we're at the point now of pulling everything together and getting into the clearance process in the near future. The issues I spoke about last month, there's a number of them of course that will require some policy discussions still within the department and within the Office of Management and Budget as well before the regulation goes out. We spoke about some these last month.

The issue of flexibility. A large number of the commenter's came in and expressed concerns about the lack of flexibility. The requirements in terms of the bar. There were certainly a lot of discussion, not only about the number of objectives, but also the percentages of the measures that were required.

The denominator issue, I mentioned that last month, that was a key issue. The ability to be able to if you attest to something with a numerator /denominator to be able to use the EHR to do that electronically as opposed to doing some of the work manually. And the applicability to state flexibility, the whole issue of how flexible could states be in setting additional requirements. There was a big concern from a number of the respondents that the states not be allowed to have too much flexibility in terms of adding additional requirements to meaningful use.

There was also quite a bit of feedback on providing additional specificity to stages two and three. A number of the respondents wanted us to actually layout the entire framework for stages two and three. They argued that it would, and of course this gets back to the discussion this morning that Paul had raised, but a number of them raised the point that this would help the vendors plan as well as themselves. And there was also some discussion about extending the stages. Some people felt that we should extend the stages, say stage three go to 2017 for example.

On the quality measures, there was also a lot of feedback on that. A large pushback on the start date. If you recall, we put in the NPRM to test in 2011 and to report through an EHR in 2012. There was a lot of pushback on that. There was a lot pushback on the measures to report in terms of their applicability to some specialties. There were some concern over the core measures and their applicability. And of course there was a number of concerns that expressed about the readiness of some of the measures that were proposed in the NPRMs, since they had not got an NQF endorsed, nor in some cases or in more cases they had not been retooled for EHR use.

Some of the other comments that came in, the hospital based eligible professional. There was a large number of comments about that, and of course that got addressed to some extent in legislation. Some people feel it got fixed "in legislation." Others are still coming in with concerns. They don't think that the legislation fixed it, at least not the way that they wanted it fixed, so that's been another interesting twist to all this.

I mentioned the multi-campus issue with hospitals last month. There's also a number of areas where there was further clarification asked within the meaningful use. There was a lot of additional comments on specific measures, clarification, whether these measures were appropriate. And then finally, the whole issue of administrative transactions. There was a lot of pushback from people who felt that that was not an appropriate criteria to be included in the meaningful use requirements.

So those are the major areas where we received comments on. So what we have done internally within CMS is vetted this in front of our senior management, both career and political. We've also been working closely with ONC staff, and also we'll be talking more with David and Farzad and others at ONC in terms of some of the potential options. And then we'll be working with our colleagues in the department and OMB over the next several months to bring this to a final rule, hopefully towards the end of spring this year. So that's kind of where we're at, at this point. It's been a lot of work by a lot of people. It's certainly been quite an effort.

Once again, I want to thank the policy committee for your input. I think it was very helpful to us as it had been NPRM. And also those who chose to comment individually or within their organizations as well. We received some very thoughtful comments and it's going to be a difficult process pulling together a final rule. It certainly won't satisfy anyone. Well it won't satisfy everyone; maybe it will satisfy a few people. But I think if people are too satisfied obviously, we haven't done our balancing act well enough and we've made a lot of friends in Congress. A number of them have expressed concerns about various parts. In fact, we're meeting with a couple of them tomorrow and there's more who want to meet with me on Friday, but we have gotten a number of interests from them. The EP issues I mentioned has already been taken care of to some extent within legislation. And basically what they did was remove the outpatient wording that was in the original statute.

There's also some discussion about fixing the multi-campus issue, although that has more ramifications, so that's still being discussed, but there could be some legislation around that. And we'll have to see what else gets people's concern. There was also a bill introduced last week by Representatives Kennedy and Murphy to extend the incentive program further and there's a little bit of additional wording in the health reform. It does a little bit of extending as well. So we'll have to wait and see how all these pan out over the next several months, but that's kind of where we're at, at this point.

So if anybody has questions or comments?

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Other than thank you very much for wading through all that and working towards the final completion.

Tony Trenkle – CMS – Director of OESS
Thank you.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Okay, David?

David Lansky – Pacific Business Group on Health – President & CEO
I'm hoping Farzad will join, I don't know if he's on by phone or he's just not here yet, but if not I can probably just carry on from here. I may ask for some help from Mariann when we get into that. So this is an update on the NHIN workgroup, and as Deven really tees up perfectly by introducing a number of the issues on the privacy and security side, which are absolutely essential to the discussions in the NHIN workgroup. And I think you'll see as we go through this a lot of dovetailing of what we're discussing and what Deven just described.

In terms of where we are, is framing the process. I think it's slowly becoming clear to me fortunately. I think what we're doing now is really elevating to this broad idea of a trust framework in just trying to articulate a recommendation to you as to what is a national trust framework look like. What are the big categories of elements of a trust framework? I would like to lay that out for you in a very high level today and have some discussion about it. Over the next month, the workgroup will try to take your feedback and their own discussions and start turning this into a recommendation letter that we would then bring back to you for discussion and hopefully at some point approval, which would then provide a basis for ONC to offer up a high-level trust framework. Then we all have the challenge of populating that framework with detail.

And I think Deven already laid out in one of the categories I'll come to some of the challenges that hopefully that workgroup will do the flushing out of the detail. So think of this as sort of starting at a high level and gradually filling out a layering of more detail, including at some point, especially when it comes to governance, saying where do we no longer speak at a national policy level because the states or local HIEs or enterprises are speaking. So that's part of the work we have ahead of us.

So let me go through this material. The slide you have in the printed packet are slightly different than the slides I'll go through here, but they're very similar in broad stroke. The committee is working around the clock to get every word right. We'll talk today about the recommendations for high-level trust framework, and then there's an illustration just to walk you through, how does this apply to the so called push model or the one-to-one exchange model as Deven's workgroup has characterized it. And that'll probably trigger some of the same discussion that we had a little bit ago with Latanya.

So our next slide, I guess I can do that. So we're talking here, we came to you a couple of months ago and talked about the role of government and we listed for you several areas where we believe government will need to play a role with a nationwide health information network. And the first of which here in red is to maintain and establish this framework of trust, including of course privacy and security protections as we just heard.

So the high level findings of the workgroup that would in effect constitute the introduction to a recommendation letter, is that there is a need for a national level trust framework to promote the electronic exchange of health information; that framework would provide a tool for understanding how trust can be implemented across a broad range of uses and scenarios. And as we just heard in Charles' example, there are many different uses and scenarios that we have to contemplate. We're not going to try to speak to them at a level of granularity, certainly on our workgroup. So we're trying to say here are the components that someone needs to address as you execute any one of these uses or scenarios.

On behalf to address the need for adequate privacy and security protections, although it's not intended. The framework's not intended to cover everything that is needed for trust and HIE. It articulates the common elements needed for exchange partners to have confidence in the exchange and recognize that those elements will vary depending upon a variety of factors relevant to each instance that we're talking

about, including who are the partners, what information is being transacted, what's the purpose of the transaction and so on.

The framework supports interoperability from a policy point of view. It recognizes there's an obligation to abide by and comply with the trust requirements in order to continue realizing the value of information exchange. So the notion here is that we all get value from these exchanges. We all have a vested interest in remaining true to the requirements so that we continue to be part of the network and receiving the value of the exchange, and obviously we want to learn from all the other HIEs that's already been undertaken around the country.

We have the overarching trust framework, the highest level we're discussing has five major components in it, and I'll lay these out a bit more in a second. A set of agreed upon business policy and legal requirements, a transparent oversight mechanism, enforcement and accountability mechanisms, a means of ensuring identity, and then a set of technical requirements that are at a minimum universally accepted. You need all five, but any one of these alone probably doesn't get you a broad trust by the public and professionals in the system.

And I would point out that the two, second and third here, the oversight and enforcement and accountability bullets take us down the road of governance, which you may recall is part of our core obligation to the developing governance mechanisms for the NHIN. It's one of our assignments from the original statute. So we will be shortly coming back to you with the beginnings of a discussion about governance issues.

I'd also mention under identity assurance, that there is now a special sub-workgroup that's been convened to go further with the discussions with NIST that we began here a month or two ago about what is the level of assurance and the mechanisms of assuring identity that we may want to come back to and recommend. So that's a special target group if you have an interest in that area.

So here are the five high-level components we are recommending. So I would say if you want to begin to think a month ahead, we will come back to you in a month and say do you agree that these are the five national components of a trust framework? So this is one you may end up needing to vote on at some point, and give us feedback now and over the next month as to whether or not you think this is right.

So first, agreed upon business policy and legal requirements, all participants in exchange will abide by an agreed upon set of rules including compliance with applicable law and act in a way that protects privacy and security to information. Second big category, that's a very big category I would say that it fits on one line, but it's actually a huge amount of policy, legal, and business expectations that have to be articulated.

Enforcement and accountability, each participant accepts responsibility for its exchange activities and answers for adverse consequences, that if there are consequences for failing to comply with the framework and the public understands that those consequences are being executed.

Oversight, transparent oversight, oversight of the exchange activities will take place to assure compliance, and the oversight process itself will be transparent to the parties and to the outside parties, the public.

The fourth category is identity assurance; this is something we began within our workgroup three or four months ago. All participants need to be ... if they're exchanging information with whom they intend and that this is verified as part of the information exchange activities.

And finally on the tactical requirements, all participants agreed to comply with some minimum tactical requirements that are necessary for the exchange to occur reliability and securely.

So then, the next set of slides lays out each of these in a little more detail. An agreed upon and mutually understood so that expectations, obligations, policies, and rules around how partners, trading partners in this case, will use, protect, and disclose health information in general, in their exchange related activities specifically. One of the controversies embedded in this language is this phase in general, and so we've used the language here to be careful to say in a sense, whatever it is, once you've received information from the exchange, you still have some obligations to communicate and be accountable for how you use that information because the other parties are expecting you to perform in a certain way.

We go back and forth between saying our job is just to discuss the exchange itself and the transitive information, but realizing that ultimately for there to be trust, the parties have to believe the other party will behave in a way that's predictable. Obviously we'll build upon this applicable state and federal law, including HIPAA. Will this framework requires participants to act in a way that protects privacy and security? And as we heard earlier, the privacy and security workgroup in our view will have to flush out what are some of the expectations that fit under this bucket number one.

And we understand that these requirements will vary upon the context of the exchange, and that I think means that we don't expect that we at a national level would lay this out in some single broad uniform way. This is going to have a lot of, the framework will describe the need for this, but it'll be developed specifically to certain context.

Enforcement and accountability, this is one of these areas of governance, each exchange partner must be accountable for its exchange activities and be prepared to answer at multiple levels. For example, the individual subjects of the exchanged information, other participants in the exchange, third parties who provide enabling functions, there may be certifiers and accrediting bodies in the loop, and obviously there are government mechanisms for enforcement.

This is meant to say that enforcement is not just conceived other than criminal or civil sanction that happens legally, but that the parties themselves may be able to detect problems in the exchange and they may opt out of the exchange as we said earlier, but that's a means of enforcement if you like, if they mistrust the infrastructure. So we're sensitive to the fact that everybody involved in this ecosystem is part of the enforcement and accountability system with differing levels of tools and authority.

There are methods for confirming, detecting, and enforcing compliance, that there are methods for doing so, and the consequences may vary at each level from something like loss of status or business relationships to an informal enforcement of penalties by government agencies and perhaps readdress if there is harm.

That the common desire to avoid these consequences and continue to be part of the exchange, continue to drive value, gives each of us some confidence that the others are going to try to play by the rules because they know the enforcement infrastructure is in place to sanction and dismiss from future valued exchanges, people who don't play by the rules.

The notion of transparency and oversight is intended to mean the management, maintenance, supervision, and monitoring of the trust relationship and the exchange activities. And we see this as a very broad opportunity for people to contribute to oversight in the exchange, much as we discussed earlier today, the opportunity for example for patients to detect mistakes in their data is a means of, as Paul described it this morning, a means of providing oversight to the quality of data exchange.

There should be as much transparency as possible in the oversight mechanisms that are used to protect information, and the oversight process and results, including findings and consequences. So the first sub-bullet suggests something like audit where we understand that there are these mechanisms in place and we have access to them as patients or professionals. And the second suggest that we get to see that there have been, oversight has been executed on behalf of protecting patient privacy.

The nature of the oversight and the mechanisms used will vary and it will depend upon the exchange model who's involved and the needs. It'll happen at multiple levels as I've said, and it should be clear that there is not a guarantee, not an absolute guarantee of privacy and security. I think we take that for granite, but we're just a reminder here that we're going to try to mitigate risk with these various mechanisms and we won't achieve perfection.

Four, identity assurance, we talked about a bit in the past, we know that none of us will exchange information with anybody out there. We have to be confident we are talking to the parties to whom we intend to communicate. Therefore, each exchange partner will need to validate and maintain an audit log of identity. And there is a variety of ways to validate the identity of parties to the exchange, and we come back to you after this workgroup does some of its work on what the appropriate mechanisms will be that we'll recommend.

And finally that there are the set of minimum technical requirements that partners have to adhere to, to support the privacy and security requirements. The technical requirements could include measures designed to ensure the data received had not been altered during transit and ideally some of this is self enforcing. Noncompliance with those technical requirements may prevent an exchange from occurring which also reduces the risk.

So that's the high-level framework that we are so far proposing to you and we'll welcome your feedback today and in the future about whether we've got that right or not.

Here, let me just quickly give you a flavor for applying it to this one-to-one exchange scenario that Deven introduced and we have been calling directive push, but I understand there's some criticism of that terminology. So we may not call it directive push for long, but it is a similar concept.

So this is one again, one of the simplest cases we so far entertained for information exchange. This is between two parties who know each other and who presumptively are qualified under HIPAA to have access to this information. We're not in this simple exchange, the person who is now custodian of my personal health information wishes to send it to somebody else who's an appropriate recipient, and the meaningful use criteria that we've recommended of course has roughly nine such instances where one party might want to send information to another party and this is the context for this immediate set of examples of illustrations.

So in number one, the agreed upon policy requirements, first of all, applicable law and the expectation of the privacy and security will be protected are in place. Secondly, there's an informal social contract that's between the EHRs, one covered entity to another without the use of a third party. So this again is the fax example, we're simply in this example, caveating the potential for abuse. This is the case in which one party is transmitting information to another known party at a known address and they have an informal understanding of who's at the other end of that receiving if you like e-mail address or Internet address.

There may be agreements required between each healthcare provider organization and its end users. So in the high ... structure we've talked about here before, we're assuming that an enterprise, a healthcare

organization is accountable for the end users within its structure and that it is representing and they did properly authenticated and identified those people within its own structure.

There may be formal agreements required if a third party is involved, depending upon what actions a third party is providing and whether they have access to data, identifiable data. For example, business associate agreements, if a third party provider in this story is providing routing or provider directory services and perhaps additional policies and agreements if they're doing other things with personal health information or metadata about it.

On enforcement and accountability in this model, we understand that exchange partners are accountable to each other, to patients, and to governmental agencies. Third parties that may be involved in this, providing identity assurance, provider directories, or secure routing should also be accountable.

One consequence for failing to uphold commitments to comply with this framework is determination of the exchange relationship between the parties. One party may cease doing business with another or cease using a routing service or some other third party that's ... that's helping the transaction take place. But other consequences obviously can include legal implications depending upon whether a legal violation or a contract breach has occurred.

And the third category, transparency and oversight, how do we detect potential violations in this case? There's governmental oversight in place presumably in terms of compliance with laws. The patient who's subject to this exchange and the exchange partners will be overseeing and monitoring to see that the exchange actually occurs as intended. There may be governmental oversight as we've discussed before, for example, certification, accreditation, or some other mechanism for the third parties who are entailed in this exchange. Those third parties may themselves play a role in oversight by being auditable for example. And that oversight must include transparency to foster accountability. None of us will know if there have been violations if we don't have some ability to see into the processes that are in place.

In terms of the last two, identity assurance and minimum technical requirements, this is a lighter environment for this one-to-one exchange. So the identities of exchange partners and/or users are primarily validated by the provider organizations or perhaps by a third-party identity provider and the other participants rely upon this. Essentially we're building out on an existing trust relationship where hospital one and group practice two already do business and know each other and have a trust relationship in their exchange today, just that this model does not overlay a new structure on top of that.

In terms of minimum technical requirements, the meaningful use certification criteria for example regarding secure transport that are already in the certification proposals would be one set of technical requirements, the ability to identify the providers electronic address to transmit information would be important, and then the ability to route information to that address which could occur in these several scenarios that are listed here. For example from an EHR to an EHR or from a lab to an EHR and so on.

So that's the overview, we have a framework with five big buckets. This is one; they gave those last few slides to illustrate how those buckets get applied to a particular scenario. This is not a recommendation, it's not meant to be precise, just to suggest to you how this would play out as we go further down the road.

So let me stop there and let me thank Mariann and others who've been very involved in the workgroup, and Farzad for providing a lot of leadership to it, and obviously everyone on the committee for helping to flush this out.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Thanks, David. Questions? I have one question, how does the work of the NHIN workgroup relate directly, indirectly, or no relationship with the HIE, the state based HIE grants? I think those are cooperative agreements or so how does that relate?

David Lansky – Pacific Business Group on Health – President & CEO
I don't know the answer yet to your question. I do know that Micky Tripathi has been working with the HIE workgroup and Deven has. We're having a collegial discussion about how to answer your question, and part of it is, what is unstated in the governance part of this trust framework is what is the governance role that we expect of these state HIEs, which are called governance entities in many cases or state designated entities. And I think the federal cooperative agreements, and maybe Jodi or someone could speak to this, with the states will prescribe some of those responsibilities at the state level and certainly we want that to be reflected in this model as it gets played out, but I don't think it's been determined fully yet.

Jodi Daniel – ONC – Director Office of Policy & Research
One of the things that clear is that what we have discussed is that the trust framework would have different layers depending on the mode of exchange use and that's consistent with some of our thinking about how depending again on what kind of roles an intermediary is taking on, there would need to be some different policies to respond to that.

I think part of what we're sort of struggling with, so NHIN is starting to look more particularly, the slides had a lot of examples of how that framework would be applied to directive push. Who's going to do the part about how the framework gets applied to this sort of bigger, more robust universe, and then we're starting to take, we are taking some of that on and particularly in the privacy and security context. So I think there's a lot of overlap here. I think we may in fact need to be more clear about who's doing what, so that it all gets done in an expeditious way.

I mean we've essentially sort of not had the IE workgroup meet because we didn't have any sort of a clear agenda beyond the lab and e-prescribing, which we weren't even done with e-prescribing quite frankly, we had the hearing, but we had just minimal recommendations that came out of it. I do think it's worth ongoing conversations, so I take some responsibility for that since I sit two-thirds or three-thirds of that equation. Part of the challenge I think is that a lot of this stuff needs to be resolved very rapidly, thoughtfully and rapidly. I'm not sure you can use those two in the same context, and we do have multiple resources at which to get at this, but it needs to be done in a coordinated way so that we're not in conflict worst of all, and best case scenario, we're coming up with a coordinated set of recommendations that apply across the setting.

Sorry, David, I didn't mean to chime in, but it's like, yes, I'm starting to see where there might be some ways to divide this pie, but it will never be in a way that's so clear cut that we can all go off in our little corners and deliberate and not be in some way, shape, or form coordinating.

David Lansky – Pacific Business Group on Health – President & CEO
I also think there's an opportunity both for bottom up and top down dialogue around this. I know because of the California experience, a lot of these issues are very much in place within California. I'm sure the other states are having the same discussions, so there's a lot to be learned for us on our committee here from what discussions and experience is occurring at the states. And then in turn, the states are often looking to not duplicate thinking and work and analysis that's already been done here or at ONC or elsewhere, so how do we disseminate whatever we determine that our discussions, so that 50 states and

50 committees don't have the same discussions without the benefit of that. So we need to do a little more I think in improving that communication loop.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Rick?

Rick Chapman – Kindred Healthcare – Chief Administrative Officer/CIO/EVP
David just asked a clarifying question and maybe we're not ready for this yet. In the discussion and the spirit of the discussion about things we should contemplate quickly about scope, and you're limiting the initial discussion to whatever word we want to use for the directive push on known entities and one-on-one, there's a stated desire incentive of both parties to cooperate under the rules.

Many of, when we go to the more robust discussion which speaks more to health information exchange as a noun is what I'd like to talk about just for a second. And before I think we go too far into it that we at least ought to state and declare what our position is on an assumption of how those exchanges, how sustainable are they going to be? And what I'm talking about is too, and I don't know what California is, but either the federal or state government, are we expecting that they, because all these initial fundings are in grants, are we expecting that they will eventually receive permanent funding via the state or federal government that will be there at the state? Because that's been kind of the question. They kind of come and go as the grants expire.

And all I would ask without as you contemplate this that we at least put an assumption about what the long-term sustainability of these heath information exchanges as a noun will be, because they're obviously the more robust and the more difficult problem to solve as it pertains to the things we've been talking about this morning.

David Lansky – Pacific Business Group on Health – President & CEO
The two quick reactions on behalf of my work in California I would say they're intended to be sustainable without significant reliance on grants. At least that's the assumption we make in California, I can't speak for the other states or nationally.

Rick Chapman – Kindred Healthcare – Chief Administrative Officer/CIO/EVP
And has that been the case at this point through charges and business relationships.

David Lansky – Pacific Business Group on Health – President & CEO
Some yes and some failures, so I think—

Rick Chapman – Kindred Healthcare – Chief Administrative Officer/CIO/EVP
Right.

David Lansky – Pacific Business Group on Health – President & CEO
But I think that the forward looking assumption is probably the case. But I think as it applies to this workgroup, it's specifically, my hope is that we collectively can identify the trust framework, which is durable and flexible, adaptable, but durable. And then whether HIE succeed or fail, given the particular models and business approaches they take, they do so without violating the trust framework or that the trust framework is more robust than the individual viability of any particular approach to HIE.

Rick Chapman – Kindred Healthcare – Chief Administrative Officer/CIO/EVP
So you're assuming that they are viable, that these guidelines will enable their lawful execution.

David Lansky – Pacific Business Group on Health – President & CEO
Yes.

Rick Chapman – Kindred Healthcare – Chief Administrative Officer/CIO/EVP
Okay.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Judy?

Judy Faulkner – Epic Systems - Founder
A couple things, one, because I've been thinking about both the NHIN and the state HIEs and it strikes me that the state HIEs just came along too quickly and shouldn't be and there should only be an NHIN, because state lines are, it's duplicative, and states lines are artificial and a lot of care across the state lines.

Number two, as we talk about identity, there's more than identity of one healthcare organization to another. They're a tricky thing of course that we really need to address is identity, at some point is identity of the patient. How do we get that straight and so if you're here, and you need to go to the emergency room in DC, and they pull your record from California, I've been told by one California CEO that if in California, even when you're trying to figure out which one is the right patient, you see more than one, you have to report it as incorrect patient information. So that was one interpretation of this, so there's a lot of different interpretations. But still I think, I don't know, I'd be curious who's subgroup is the patient ID under as we deal with all this?

Deven McGraw – Center for Democracy & Technology - Director
I think it's under ours, Judy. We had it on the long-term work plan.

Judy Faulkner – Epic Systems - Founder
We do?

Deven McGraw – Center for Democracy & Technology - Director
Yes.

Judy Faulkner – Epic Systems - Founder
Okay.

Deven McGraw – Center for Democracy & Technology - Director
Jodi agrees with me.

Judy Faulkner – Epic Systems - Founder
Okay. Good.

Latanya Sweeney – Laboratory for International Data Privacy – Director
It's kind of interesting, because it's a really big important issue, but you can't get there by one-to-one thinking. So that's what I meant by you can't stay in this one-to-one model, because you're not going to get there with these parts.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Judy on this point or Art? Is yours on this point? Okay, so Art? Alright, David you want to ...

David Lansky – Pacific Business Group on Health – President & CEO
The last point that Latanya made, it occurs to me that back to the 50 states question, there may be some states which will work much more actively to address a solution to the patient identity and record locater service model and other states that will not. We should have kind of a surveillance mechanism here to learn what we can from those states that choose to go down that path more actively so we can do that.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Art?

Art Davidson – Public Health Informatics at Denver Public Health - Director
Yes, I want to thank the group, I think you're making progress even though you may not feel that, David, and I think it lines up well with what Deven described earlier. This morning we had a really well presented and extensive around the privacy and security and how there needs to be some sort of reporting mechanism, some method by which that is achieved for patients or institutions that find that there's been a problem.

I wonder in this oversight and transparency and enforcement activities that you discussed whether you had any idea about what that would be like for when someone feels like there's not been the type of adherence to their policies that are being set forth and to whom that would be. Is that the Office of Civil Rights? Where would that be?

And I ask that because we describe ourselves as promoting a learning health and healthcare system, and if it goes to OCR, is that really going to help other states figure out where there may be issues to deal with or other communities that could learn from some oversight commission, omission, whatever, where there's been a problem in adhering to the proposed policies?

David Lansky – Pacific Business Group on Health – President & CEO
The short answer is we haven't had that discussion. I think it's just naturally we did discuss at a one level up from there that we can develop a structured way to think about the alternative means of oversight and enforcement recognizing as the slides indicated that there are many layers in modality.

And one, I appreciate what you're suggesting and particularly that there's sort of a learning system opportunity here that capturing the observed problems with maintaining trust violations if you like will be if we can capture and disseminate that we can help everybody improve their systems more broadly and not just have it go into some formalistic sink. So that's something we should give some thought to if we go further.

Deven McGraw – Center for Democracy & Technology - Director
I have question, in an early set of slides where it indicated that the privacy and security workgroup was going to address privacy and security information once the information is received, and I think it's a rather narrow conception of our charge. So I just ask that it be deleted.

David Lansky – Pacific Business Group on Health – President & CEO
From all historical documents.

Deven McGraw – Center for Democracy & Technology - Director
Never to be heard from again.

David Lansky – Pacific Business Group on Health – President & CEO
Thank you. They're all ...

Deven McGraw – Center for Democracy & Technology - Director
Unlike health information, we can delete. Yes, no, just in the context. I mean clearly we're going down the pathway of thinking about what protections need to be in place when data's exchanged and not just what happens after it's been received.

David Lansky – Pacific Business Group on Health – President & CEO
Yes.

Deven McGraw – Center for Democracy & Technology - Director
Going back to the conversation earlier where we are sort of dealing with this core set of issues and multiple workgroups, we can just continue to coordinate well on that.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Jodi?

Jodi Daniel – ONC – Director Office of Policy & Research
Thank you. And I agree with what Deven said, that was sort of my reaction too, so that's a major point, just based on the discussions that the workgroup has been having. One, I just want to commend the workgroup. I think this is actually really great work, and I think the concept of trying to come up with a durable trust framework that could apply across a variety of different models, but then trying to dive into one particular scenario where it's kind of a little bit more pressing right now, I think is great. And I think can help us in the future as new models are developed, as things become kind of moved from said direct model, etc.

The one thing I would suggest, and I think you're probably having these conversations, I've been in and out of some of the meetings, but is that it would really be helpful to have some recommendations or some thoughts from the workgroup on what should be the federal role in all of this versus where we can defer to the states versus where it's really a business rule or up to each individual organization that is trying to exchange information to figure out.

And then also, both from a standpoint of where should we set the line in the sand of this is the expectation of what people should be doing, and then as well as where we can provide either guidance to states as our grantees or we can provide guidance in the form of here are some things you should think about if you're having participant agreements as part of your business approach, organizational approach. So not just where we would regulate or set the rules, but also where we might be able to be helpful to either provide some guidance and best practices, that sort of thing.

One point I think somebody made, I can't remember who about the issues here are kind of too high a number to count and we're never going to think of every scenario and every model and every permutation of all of that, to the extent that there are some criteria that we can use so that as the new model comes down the pike three years from now or as a new use of data comes down the pike, we might be able to evaluate it against subjective criteria; that could be helpful since the workgroup can't possibly come up with every scenario that may exist or may ... in the future. I think that could be really useful in kind of flushing out the trust framework for exchange. So that's just some things that I think might be useful.

We do have just for folks, refreshing people's memory, the high-tech legislation does in fact give ONC responsibility for establishing a governance mechanism for the NHIN and that's pretty much what the language says, it's really that broad; which leaves both a lot of flexibility, but does present an obligation to us, so any sense of government role and what that might look like would be helpful. We have been

advised that we would need to do that for regulation, that we would need to have a governance mechanism for regulation. So some piece of that would probably be regulated, but that doesn't mean that everything we do would be regulation.

David Lansky – Pacific Business Group on Health – President & CEO
I think our hope by let's say June to have the first high-level views of what some of those approaches might be.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Charles?

Charles Kennedy – WellPoint – VP for Health IT
I want to compliment the workgroup for making progress in a difficult area, and with that buttering up, ask them to consider one other thing. A lot of health plans have used the clinical aspects for claims data and have then begun through an algorithm against them to identify gaps in care. And we typically use that data to try and influence the patient toward getting your hemoglobin A1C check, whatever it might be.

However, reaching the physician with that information has been a challenge. We typically do it through the practice management system. And I was wondering if the subcommittee could consider, would it be an appropriate use of this approach, the NHIN direct push approach for a health plan to be able to push a gap in care alert as part of an exchange of data. And I know that opens up a fair number of issues, but I'd like the committee to consider that please.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Neil?

Neil Calman – Institute for Family Health – President & Cofounder
I just wanted to make a request that at the next meeting that we get an update from the HIE workgroup. I think that we need—

W
...

Neil Calman – Institute for Family Health – President & Cofounder
What?

W
...

Neil Calman – Institute for Family Health – President & Cofounder
I think that what we're understanding in all of this is that there's a lot of interplay between these things and I think we have to continue to move in parallel tracks, maybe I'm making a recommendation that you meet and then report back. But I guess my real concern about this is, it goes back to David's comment about what's going on in California and you say, well, some of them are going to survive and some of them aren't. And all I keep thinking about is how I really believe in this stuff about interoperability and its importance in improving patient care and safety and it's not okay with me if the western part of New York can't do that at some point because their HIE just couldn't develop a business model and collapses. I mean somehow we're sort of dependent upon these organizations.

We've created a model for this, not for the push model, but for the more advanced levels of exchange. We have a model that's dependent upon the survival of these organizations, so I think that their survival becomes something that we need to discuss. And if in fact we're not secure about that in a more general way across the country, we sure as heck should be looking at other models, the data banking models, other kinds of models to say how come we're focused on this one model and yet at every single meeting, people keep talking about how it might not survive and they are not all going to survive? I just keep wondering about what's happening to the people who live in those areas? And we need alternative models if we're going to really think about exchange in a more global sense.

So I would like to see those things continue to evolve, because I think when those discussions come back to the table here, it's going to become clear that we need to broaden our thinking about the various ways in which those exchanges are going to take place at a higher level.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Latanya?

Latanya Sweeney – Laboratory for International Data Privacy – Director
Yes, so I always come back with these out of the box comments. So normally, kind of like what Neil was saying, so normally when we think about, normally if you were to ask a computer scientist to think about trust, they start with the players. Because at the end of the day, the patient has to believe in the system or they're going to want a consent, they're going to want to opt out, blah, blah, blah, the provider has to trust that they have a complete record, they're not going to be overwhelmed, or underwhelmed.
They have to believe that the HIEs are going to be there or they might lose some information or what have you. And the ingredients of the trust framework that are put here are policy oriented, not the kind of, it's a different kind of trust issue.

And I was wondering if you guys have thought about it and chose this way because it fit better for the policy relationships or whether it's something else to think about?

David Lansky – Pacific Business Group on Health – President & CEO
We've actually discussed the non-policy component a fair amount, but not much more than postulated. And that is, we haven't proposed actions on behalf of the federal government or other policy players to influence or enhance it.

Latanya Sweeney – Laboratory for International Data Privacy – Director
No, what I mean is like for example if I focused on the individual players, as soon as I say providers, the liability is a big issue. Are they going to trust that that information is accurate? Are they going to still order more tests because they're risk adverse to and so forth? So it's a totally different set of problems to address, some of them are policy things to address, but in some sense they don't get captured here and I worry about that.

David Lansky – Pacific Business Group on Health – President & CEO
Did something strike you as a way to recast these five buckets that would do better at providing us a place to have that discussion?

Latanya Sweeney – Laboratory for International Data Privacy – Director
Well it's just a total rethinking, right?

David Lansky – Pacific Business Group on Health – President & CEO
Yes.

Latanya Sweeney – Laboratory for International Data Privacy – Director
It's like sort of saying, let me start with the people and say what are their issues? What does it take for them to trust the system? I don't know. They may flush out some of its got to portion to the same bucket.

David Lansky – Pacific Business Group on Health – President & CEO
It's a very good suggestion, we'll take another look at the groupings and see whether it addresses that.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
I have question, I'm not sure who to ask though. It has to do with meaningful use in this area. So in our third category, care coordination, it clearly requires data exchange, information exchange, and I don't know whether that now in NPRM is exchange with a small e or big e. So with a small e, it might be what you call the directive push or the one-to-one, in the big e, it might involve all the things that you're trying to create, and I don't know. At least in stage one, fortunately we just have to have the capability to do something. Clearly by 2013, it's going to have to have an exchange and I just don't know whether these policies, the framework, etc. will be baked into that requirement in order to satisfy meaningful use and whether that's being discussed somewhere. I don't know whether that's in the HIE group or the NHIN group.

David Lansky – Pacific Business Group on Health – President & CEO
I would say that like in today's simple example, we have contemplated taking the requirements, let's imagine, proposed stage two requirements for meaningful use, which in gender, data exchange and collaboration, care coordination. It would be natural to take those and drive them through this framework and see where the gaps, where the policy holes, or other—

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
But on the flip side that the provider then have to comply, adhere with all of the policies that your group with come up with in order to qualify as the exchange with the big e. It's not clear from the NPRM, is anybody else clear whether that's invoked?

M
...

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Well, yes, it's more than just whether HIE is a noun or a verb, it's whether exchange has with it, exchange complying with all of these policies.

Latanya Sweeney – Laboratory for International Data Privacy – Director
I mean I don't think that's at all explicit in the rule—

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Right.

Latanya Sweeney – Laboratory for International Data Privacy – Director
Because and in part, because it's only a test, and the test doesn't even have to be successful.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Right.

Latanya Sweeney – Laboratory for International Data Privacy – Director

Right, late in the proposal.

Deven McGraw – Center for Democracy & Technology - Director
Yes, and recall that the privacy and security workgroup specifically identify that the security functionalities that were in the certification IFR were not necessarily required to be utilized. They all touch on what are called addressable requirements under the HIPAA security rule which essentially we asked that in fact providers address how they're going to use them as part of meaningful use, that that was a comment that we made to the NPRM, it's not part of the NPRM today.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Okay, so it's not part of the deliberations at this point, but it may be premature.

Deven McGraw – Center for Democracy & Technology - Director
I mean I do think it's vague right now what it says, but because the NHIN workgroup is looking at the direct one-to-one, whatever we want to call it, exchange based on the types of exchange for a meaningful use, that it does beg the question of how do we make this happen is that part of meaningful use or is that imposed another way or what does that actually mean?

And I think Christine's right for 2011 at least, the way it's proposed less of an issue, but going forward I think it does become an important question.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
And back to the 18-month discussion, we're going to actually be dealing with and hopefully find some way of signaling the community and industry by the end of this calendar year. And so we would want to wrap clearly your work or wherever it's collectively amongst the three workgroups dealing with this, what should be in the meaningful use criteria for care coordination in 2013?

David Lansky – Pacific Business Group on Health – President & CEO
Correct.

Deven McGraw – Center for Democracy & Technology - Director
So in other words hurry up.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Hurry up, and be clear and explicit.

Deven McGraw – Center for Democracy & Technology - Director
And thoughtful.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
And thoughtful. Judy, I think you were—

Judy Faulkner – Epic Systems - Founder
You may need some good terminologies, higher level, lower level is what Neil was using, but there may be some others that we might want to come up with to represent those that have a kind of intermediate repository from those that are doing direct exchange, perhaps those are the words.

The second thing I was going to talk about was just when Neil was talking about viability, those with an intermediary repository, I think there are two ways that they can survive financially, one is to charge the healthcare organizations, and the other is to sell the data. And I think those are the only really true viable

ways. And then if we are addressing their viability, we really then need to begin addressing the sale of the HIE data to pharmas, to payers, etc.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
It's on Deven's long list, that she ...

Deven McGraw – Center for Democracy & Technology - Director
It's on our long list, you're on my workgroup.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Yes, right.

Judy Faulkner – Epic Systems - Founder
But I wanted to make it clear what we're talking about when we're thinking about—

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Yes.

Judy Faulkner – Epic Systems - Founder
How do we deal with that viability?

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
That's right.

Judy Faulkner – Epic Systems - Founder
I guess there's a third way, which is government sponsored.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Right, we ruled that one out with the recovery act. Any other comments, questions? Thank you, David. Now I think we're ready to open it up to the public for comments and questions.

Judy Sparrow – Office of the National Coordinator – Executive Director
That's right. Anybody in the audience cares to make a comment, please come up to the microphone, which will be here momentarily, and on the telephone if you want to make a comment push star one, and if you're on the Web, please dial 1-877-705-6006. Please state your name, your organization, and it's a three-minute time limit.

And in the room we have somebody for Deborah.

Deborah Peel – Patient Privacy Rights
Hello, everybody, Deborah Peel with Patient Privacy Rights. It's nice to see you again. I'm going to try to talk fast for three minutes. We're talking about the high level, part of the complexity of everything that you all are trying to address is because we have what we have. If we're going to think at a high level, we need to think about where we are going.

And where we're going is, I'm going to use Don Berwick's idea, is patient empowerment. As he said in his paper, the data should belong to the patients and others should have to ask for it. And if we understand that we have to, we have to, and I think that we will in this country move to that system, because we're a nation of individuals with individual rights. And so what we've got now is some pretty bad stuff because

it's been there, and it's really important not to grandfather these kinds of things in. So there's a lot of things to think about.

One is the fact that you know this I'm sure, recently in the UK they had to stop moving data from individual practitioners offices to the NHS because they used opt out and when the public finally figured that out, that they had to opt out of the system, they got angry, and the data transfers been shut down. And many of you have emphasized today the importance of the ability to segment information. We will never get trust and we will never get people to put the data in unless it can be segmented, and thank you, Charles, you probably know this, I'm a psychiatrist, and the problem that you're talking about with Lithium is absolutely true and we have to give our patients Miranda warnings. If you take this medicine, it cannot be kept private, and so what we have is without privacy people foregoing essential medicines. And some others have talked about, a lot of states have decided to just not even try with sensitive information.

I really think that you all are coming very close to understanding the need to require all of these systems to be able to segment information according to the patient's wishes, because that's in state laws and that's what people expect, that's the Tang test, people expect to be able to segment their data. When we get to use technology fully where individuals can make these decisions for themselves, we're not going to be needing to make these policies for them. We'll be able to teach them about the choices and they'll be able to make the jobs. And no one, I really think in listening to you, you're agreeing that no one should have to be all in or all out and have to forego the benefits of technology because they can't trust the systems. People should be able to selectively share their data with whom they want, that's the way it's always been.

In terms of your emphasis on oversight, patients could not agree more, we do need oversight, but how are you going to have that without accountability? Where does that come from? Audit trails. What have we done in meaningful use? We've pushed them back and health technologists are saying, well, we can't do them, but that isn't true. The people that do authentication are now saying, if we authenticate all the thousand people on the staff at Seton Hospital in Austin, Texas, it's really more like five, then you know what, we know who got into which record on which day and probably for which purpose because we know maybe their role.

So actually audit trails can be created very easily right now using the kinds of robust authentication trails that are created when certain staff members log into records. So if we're going to ever have accountability, there needs to be audit trails for every disclosure of PHI, which we think that we got into the stimulus bill, that's pretty much what our coalition thought was put in there, and so we'd like to see that, and that obviously means re-disclosures and re-disclosures and so on all have to be tracked as well.

Let me think, I've got so many notes here, regarding e-prescribing, the situation where it's a danger when other doctors don't know. As a psychiatrist I've faced that problem for 35 years. Many patients don't want their other doctor to know about the medicine because the other doctor is prejudiced against them. And I've certainly seen this many times with my own patients, as soon as somebody knows they're seeing a shrink, they're like everything's in that person's head, and so I end up being the internist, that's not a good solution. It's not a good solution.

The other thing is about the other side of that with internists, internists are not stupid, cardiologists in particular, they're going to say by the way are you taking something that might interfere with medicines for your heart, like are you taking an antidepressant? You've got to tell me this because I don't want to make you sicker, I don't want to make you die. Cardiologists are not stupid.

In other words, we don't need to destroy people's privacy because we think that the doctors are too dumb to ask the right questions. Cardiologists are very aware of what kinds of things conflict with a medicine and they would be I don't know remiss or even potentially committing malpractice if they didn't explore those things specifically with a patient. So as a practicing physician, I have to say I don't think technology has to solve all the problems because it's really our responsibility to fair it out. Hey, did you forget something, to tell me that, I know you filled out all this stuff, but tell me now, this is for real. It's really important not to forget the way that practice actually works.

And then in terms of health information exchange, David, I think your five principles are only okay if we again put the patient's wishes into that and make that the sixth thing, because it's so clear what people expect, and they certainly don't know what a HIE is. I mean those of us who really care about data being exchanged and data being available for research, which we do, we barely can figure out what's an HIE or an HIO. I mean there's no way the public knows this.

And in the future, we're going to have to have a single place for patient empowerment where we can set directives and choices about what happens. We've got to look toward that future. So when we have the ability of the patient to make those decisions, then kind of the paternalistic industry current situation driven place we are now where we're having to try to figure out how to build trust into these untrustworthy systems, that's going to go away if these systems are required to truly meet existing state laws and ethics.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you, Deborah.

Deborah Peel – Patient Privacy Rights
You're welcome.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Thank you.

Judy Sparrow – Office of the National Coordinator – Executive Director
Dr. Tang?

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Anymore?

Judy Sparrow – Office of the National Coordinator – Executive Director
No.

Paul Tang – Palo Alto Medical Foundation – Internist, VP & CMIO
Okay, very good. Well thank you for another productive meeting and we keep making progress. We're not avoiding the tough issues. We still have lots of work on the workgroups, and look forward to seeing you next month when we continue our journey. Thank you.

Public Comments Received During the Meeting

1. What is direct outreach to consumers to ensure they understand the trust framework?

2. Identity Assurance in Trust Framework is limited to assurance that providers electronic address is correct and the person's identity is assured. That is Fine for Providers. Where is the additional information required by PATIENTS to feel confident that the exchange was between parties that they - the PATIENT - can identify when they review their records?

3. Great Discussion about What data and consumer consent is allowed. However what is not addressed in the discussion concerns what data about the PROVIDER is going to be made available to the Patient. Who addresses from a POLICY issue what data, level of detail including provider location, practice relationship, contact information SHOULD be shown to the consumer?